Cellebrite
PHYSICAL ANALYZER

Logical Analyzer and UFED Cloud

User Manual

May 2021 | Version 7.45

Cellebrite

Legal notices

Copyright © 2021 Cellebrite DI Ltd. All rights reserved.

This document is delivered subject to the following conditions and restrictions:

- This document contains proprietary information belonging to Cellebrite DI Ltd. Such information is supplied solely for the purpose of assisting explicitly and properly authorized users of the Physical Analyzer.
- No part of this content may be used for any other purpose, disclosed to any person or firm, or reproduced by any means, electronic or mechanical, without the express prior written permission of Cellebrite DI Ltd.
- The text and graphics are for the purpose of illustration and reference only. The specifications on which they are based are subject to change without notice.
- Information in this document is subject to change without notice. Corporate and individual names and data used in examples herein are fictitious unless otherwise noted.

Contents

1. Introduction ____ 14

1.1. Physical extraction ____ 14

1.2. Data analysis ____ 15

2. Installation and activation ____ 17

2.1. System requirements ____ 17

2.2. Installing the application ____ 18

2.2.1. Silent installation ____ 23

2.3. Activating the license ____ 24

2.3.1. New version notification ____ 24

2.3.2. Using a dongle license ____ 25

2.3.3. Using a network dongle license ____ 27

3. Scanning for malware ____ 29

3.1. Updating the signature database (online) ____ 30

3.2. Updating the signature database from file (offline) ____ 31

4. Getting started ____ 33

4.1. Starting Physical Analyzer ____ 33

4.2. Opening an extraction for analysis ____ 33

4.3. Using the case wizard ____ 34

4.3.1. Starting the case wizard ____ 35

4.3.2. Loading evidence ____ 36

4.3.3. Examination tools ____ 69

4.4. Analyzing multiple extractions ____ 70

4.4.1. Opening and merging projects 71
4.4.2. Extraction Summary 72
4.4.3. Renaming projects and extractions 73
4.4.4. Decoding and analysis 74
4.4.5. Multiple extraction settings 75
4.4.6. Reporting 75
4.5. Saving a project session 76
4.6. Adding external files 77
4.7. Loading a project session 79
4.8. Closing a project 79
4.9. Closing Physical Analyzer 79
4.10. Keyboard shortcuts 80
5. Orientation to the workspace 81
5.1. Navigation menu 81
5.1.1. Home 81
5.1.2. Timeline 82
5.1.3. Analyzed data 89
5.1.4. File systems 90
5.1.5. Insights 92
5.1.6. Tags 93
5.1.7. Reports 93
5.1.8. Cloud 94
5.1.9. Managing project actions 95
5.1.10. Viewing extraction data from multiple projects 96

5.2. Data display area 96

5.2.1. Welcome tab 97

5.2.2. Extraction summary tab 98

5.2.3. Data tabs 106

5.2.4. Notifications center 122

5.3. Viewing image files 124

5.4. Viewing docs in Physical Analyzer 128

5.5. Viewing video files 130

5.6. Redact content 133

6. Locating and analyzing information 135

6.1. Searching for information in a data tab 135

6.2. Using the quick filter 135

6.3. Using the advanced filters 139

6.4. Using advanced search 139

6.5. Searching for information in all open projects 140

6.6. Browsing the file system 142

6.7. Accessing conversation view 142

6.8. Working with watch lists 145

6.8.1. Creating a watch list 145

6.8.2. Editing a watch list 147

6.8.3. Importing a watch list 147

6.8.4. Exporting a watch list 148

6.8.5. Deleting a watch list 148

6.8.6. Running a watch list 149

6.8.7. Locating a watch list 151

6.9. Importing and categorizing hash sets 152

6.9.1. Managing hash sets 153

6.9.2. Adding a hash set 156

6.9.3. Running hash sets 158

6.9.4. Editing, updating and deleting hash sets 162

6.9.5. Exporting the hash database 163

6.10. Tags 167

6.11. Device locations 170

6.11.1. Viewing online maps 171

6.11.2. Viewing offline maps 174

6.11.3. Markers and information windows 177

6.11.4. Enrichment of BSSID and cell IDs 178

6.11.5. Retrieving addresses 181

6.11.6. Decoding and analyzing drone data 182

6.12. Recording screen captures and video 186

6.12.1. Screenshot 186

6.12.2. Video 188

7. Translating decoded data 191

7.1. Smart Translator 191

7.1.1. Installing the Smart Translator languages 192

7.2. Basic translation pack 197

7.2.1. Installing the Basic translation pack 198

7.2.2. Selecting the languages in MyCellebrite 202

7.3. Using the feature 204

7.3.1. Reporting 206

8. Cloud extractions 208

8.1. Extracting private cloud account data 208

8.1.1. Adding case details 209

8.1.2. Selecting data sources 211

8.1.3. Validating cloud account credentials/tokens 214

8.1.4. Managing cloud extraction settings 217

8.1.5. Viewing the summary before extraction 218

8.1.6. Monitoring extraction progress 219

8.1.7. Multi-factor authentication and CAPTCHA 220

8.1.8. Password collector 223

8.1.9. Choosing from multiple Google accounts 224

8.1.10. IMAP parameters 225

8.1.11. Advanced options 226

8.1.12. Cloud Login Collector 233

8.1.13. Exporting an account package from Physical Analyzer 233

8.2. Extracting public cloud account data 234

8.3. Supported content 239

8.3.1. Supported apps by extraction method 243

8.3.2. Cloud Login Collector: Supported tokens & OS 246

8.3.3. Content categories 247

8.4. Troubleshooting 248

8.4.1. Restarting the UFED Cloud Communication Manager Service 248

8.0.1. Known issues and limitations 249

9. Generating a report 257

9.1. Report dataset settings 259

9.2. Report security settings 262

9.3. Report layout settings 263

9.3.1. Formatting the UFDR file 266

9.4. Generating a Preliminary device report 268

10. Performing extractions 269

10.1. Extraction from iOS devices 269

10.1.1. Physical extraction 270

10.2. Extraction from GPS or mass storage devices 277

10.2.1. Reading data from a GPS or mass storage device 278

11. Advanced features 280

11.1. App insights 281

11.1.1. Extraction summary 281

11.1.2. Installed Applications 281

11.1.3. Table view 284

11.2. AppGenie 285

11.3. Virtual Analyzer 288

11.3.1. Online/offline mode 289

11.3.2. Virtual Analyzer notes 290

11.3.3. Installation process 291

11.3.4. Using the Virtual Analyzer 294

11.3.5. Emulation options 299

11.4. Accessing public data 300

11.4.1. Extracting the data 301

11.4.2. Creating a public domain avatar 305

11.5. SQLite wizard 307

11.5.1. Identifying a database 308

11.5.2. Building the query 311

11.5.3. Mapping data 321

11.5.4. Running the created query 327

11.5.5. Managing queries 328

11.6. Fuzzy models 330

11.7. Generating dictionary files 333

11.8. Working with TomTom 334

11.8.1. Exporting a TomTom file 334

11.8.2. Importing a TomTom file 335

11.9. Opening an encrypted extraction 336

11.10. Opening an encrypted zip file 338

11.11. Extraction and decryption of BlackBerry backup files 339

11.12. WhatsApp decryption on BlackBerry databases 340

11.13. Exporting an account package from Physical Analyzer 345

11.14. Media classification 346

11.14.1. Running Media classification 347

11.14.2. Viewing and analyzing classified media 349

11.14.3. Running Media classification on demand 352

11.15. Selective apps decoding 353
11.15.1. Selecting apps to decode 353
11.16. Carving images 357
11.16.1. Scanning for carved images 357
11.16.2. Working with carved images 359
11.17. Carving locations 361
11.18. Generic file carver 363
11.19. Verifying hash values 364
11.20. Accessing WhatsApp Web data 365
11.21. Network dongle – admin procedures 369
11.21.1. Network dongle – system requirements 369
11.21.2. Managing network dongle licenses 369
11.21.3. Features page 370
11.21.4. Sessions page 371
11.21.5. Updating the network dongle license 371
11.21.6. Standalone installation of the required drivers 372
11.21.7. Enabling network dongle logs 373
12. Working with hex data 375
12.1. Searching for information in the Hex data and decoded data 376
12.1.1. Searching strings 377
12.1.2. Searching bytes 379
12.1.3. Searching dates 381
12.1.4. Searching SIM ICCID numbers 384
12.1.5. Searching SMS numbers 386

12.1.6. Searching for regular expressions (GREP) 388

12.1.7. Searching SMS text strings 391

12.1.8. Searching for patterns 393

12.1.9. Searching for codes and passwords 396

12.2. Browsing the hex extraction 398

12.3. Using an offset to jump to a different location in the file 398

12.4. Working with Hex tags 398

12.4.1. Adding a Hex tag 399

12.4.2. Editing a Hex tag 400

12.5. Decoding raw data 400

12.6. Viewing the hex data information 401

12.7. Locating specific data types in the Hex 402

13. Camera and screenshot evidence 403

14. Advanced decoding 404

14.1. Managing chains 404

14.1.1. Constructing a new chain 406

14.1.2. Editing an existing chain 407

14.1.3. Attaching devices to a chain 409

14.1.4. Setting the default device chain 410

14.1.5. Detaching devices from a chain 411

14.1.6. Removing a chain 412

14.1.7. Chain descriptions 413

14.2. Plug-ins 416

14.2.1. Managing plug-ins 416
14.2.2. Running a specific plug-in 418
14.3. Using the Python shell 418
14.4. Exporting the file system 419
14.5. Using the Android unlock pattern carver plug-in 419
14.6. Android unlock password carver plug-in 420
15. Settings 421
15.1. General settings 421
15.2. Data files 429
15.2.1. Data files filtering methods 430
15.2.2. Managing data files settings 430
15.3. Hex viewer 432
15.4. Models 433
15.5. Timeline 434
15.6. Interface 435
15.7. Additional report fields 436
15.7.1. Adding a new report field 436
15.7.2. Editing a report field 437
15.7.3. Deleting a report field 437
15.8. Report defaults 438
15.9. Cellebrite Commander 442
15.10. Post-chain plugin 444
15.11. Saving settings 445
15.12. Loading settings 445

15.13. Setting project settings 445

15.13.1. Setting a unified time zone for the project 445

15.13.2. Setting the case information 447

16. Menus 449

16.1. File menu 450

16.2. View menu 451

16.2.1. Viewing the trace window 451

16.3. Tools menu 452

16.4. Cloud menu 453

16.5. Extract menu 454

16.6. Python menu 455

16.7. Plug-ins menu 456

16.8. Report menu 457

16.9. Help menu 458

17. Glossary 459

18. Index 468

1. Introduction

Cellebrite UFED is made up of a number of components:

- Cellebrite UFED (Touch and 4PC) and Cellebrite Responder enables logical, password, SIM, file system, and physical extractions from mobile devices, which can then be saved to a USB flash drive, SD memory card, or directly to your PC.
- Extractions from cloud-based data sources. Cloud data sources refers to services provided to consumers over the Internet.
- Cellebrite Pathfinder enables you to immediately identify the links between persons of interest and pinpoint the connections and communication methods used between multiple devices, based on reports generated from physical, logical, and file system extractions.
- The Physical Analyzer application provides an in-depth view of the device's memory using advanced decoding, analysis, and reports. Physical Analyzer can decode all types of extractions created by UFED.
- The Logical Analyzer application reads UFED files (UFED dump files *.ufd) and UFED report (*.xml) files created as part of the logical extraction.
- The Phone Detective application helps investigators quickly identify a mobile phone by its physical attributes, eliminating the need to start the device and the risk of device lock.

The UFED work flow consists of two steps:

- Extraction - Physical, file system, logical, password, SIM card extraction using UFED.
- Decoding, analysis, and reporting using Physical Analyzer or Logical Analyzer.

This manual is for both Physical Analyzer and Logical Analyzer. Logical Analyzer includes a small fragment of the Physical Analyzer capabilities. Features that are only applicable to Physical Analyzer are indicated. If you upgrade from a logical license to an ultimate license, the software will be upgraded to Physical Analyzer.

This manual also describes the UFED Cloud extraction feature. UFED Cloud assists law enforcement agencies and enterprises to enhance their investigations by extracting and displaying information from cloud-based data sources. To use UFED Cloud within Physical Analyzer, a separate license in required.

1.1. Physical extraction

When performing a physical extraction, UFED uses advanced extraction methods to create a single Hex extraction file for each flash memory chip, or address range utilized by the mobile device. Unlike logical extraction processes, the method of the physical extraction is to bypass the device's operating system, and to acquire the data directly from the device's

internal flash memory. The device memory is captured into Hex extraction file(s) that are later read and decoded using Physical Analyzer.

The created physical extraction includes memory space unallocated by the device's OS which may contain deleted data such as Instant messages, call logs, phonebook entries, pictures, videos, and user passwords.

Physical extraction provides a bit-by-bit copy of the entire flash memory of a mobile device. Decoding of physical extractions not only enables the acquisition of intact data, but also data that is hidden or has been deleted. Deleted data can be recovered from files and unallocated space[1].

Physical Analyzer provides advanced carving algorithms, by recovering SQLite records to reveal additional deleted data from unallocated space. The amount of deleted data varies depending on the data on the device. The decoded data is displayed in the same lists as the analyzed data. For example, deleted Instant messages from unallocated space are displayed in the same list as the Instant messages.

Data carving from unallocated space provides the following benefits:

- Best and quickest solution for uncovering deleted data on the market.
- Reveal additional deleted data in less time.
- Reveal deleted data that was not available previously.
- Reveal higher quality data - both false positives and duplicates are automatically removed.
- Automatic activation: There is no need for manual activation.
- Various content types supported such as: Instant messages, Calls, Contacts, Emails, and application data[2].
- Same view: Ability to arrange all data, including data decoded from unallocated space, in the same views and with timelines.

1.2. Data analysis

Physical Analyzer enables the investigator to perform in-depth analysis of the extracted data and generate reports.

Physical Analyzer has the following key features:

- Decoding of the extraction with a layered view of memory content

[1]Unallocated space is clusters of a media partition that is not in use for storing active files. It may contain pieces of files that were deleted from the file partition but not removed from the physical disk.

[2]Application data such as: Kik, WhatsApp, Facebook, Facebook Messenger, Twitter etc.

- Provides a detailed view of the Hex file
- Reconstructs the device file system
- Decodes various Analyzed data types such as: Contact lists, Instant messages, call logs, device information (IMSI, ICCID, user codes), application information, and more
- Provides a view of data files – images, videos, databases, and so on
- Provides access to both current and deleted data
- Reveals device passwords (when applicable)

- Machine learning algorithm that automatically categorizes all images in a case to help quickly single out places, faces, and objects to help find connections faster.
- Powerful extraction for iOS and GPS devices
- Intuitive and user friendly UI for browsing the extracted information
- Powerful analysis and search tools
  - Instant search for all project content
  - Advanced search based on multiple parameters
  - Instant search for data tables content
  - Watch lists for automatic highlighting of information based on a predefined list keywords
  - Timeline for viewing all the events performed via the mobile device in a single chronological view
  - Malware scanner identifies malware in the device
  - Search the Hex by various parameters such as strings, bytes, numbers, dates
  - Ability to use regular expression search (RegEx) to look for specific data strings
- Tag memory locations for indexing of key areas for later review
- Use Python shell commands for data analysis
- Plug-ins
  - Add or remove plug-ins
  - Write your own plug-ins using Python scripting language
  - Manage chains
- Generates customizable reports (logo, header, etc.) in multiple formats

2. Installation and activation

This section describes the installation and activation process of Physical Analyzer on your PC.

2.1. System requirements

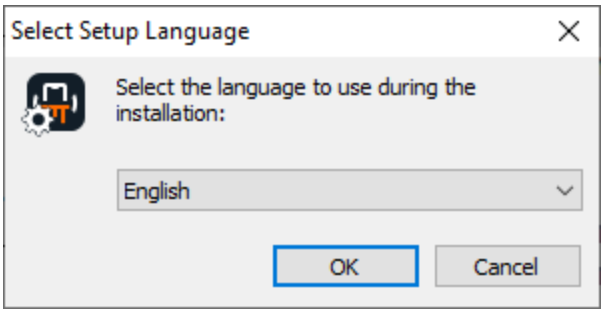
PC	Windows compatible PC with Intel i5 or compatible
CPU	4 cores
Operating System	Microsoft Windows 10, 64-bit Microsoft Windows 8.x, 64-bit
Memory (RAM)	16 GB
Space requirements	500 GB of free disk space for installation and highlights database SSD recommended
Graphics Processing Units (Recommended)	NVIDIA® GPU card with CUDA© compute capability 3.5 or higher). See the list of CUDA-enabled GPU cards. *The GPU is recommended to boost the speed of processing the CSA category in the Media classification engine.
Additional Requirements	Microsoft .Net version 4.6.2 Windows Media Player (default version for installed OS or higher) to use the Capture tool and play video playback.
Permissions	If you intend to activate the application using a hardware license key (dongle) provided by Cellebrite, you must have administrative rights over the computer.

2.2. Installing the application

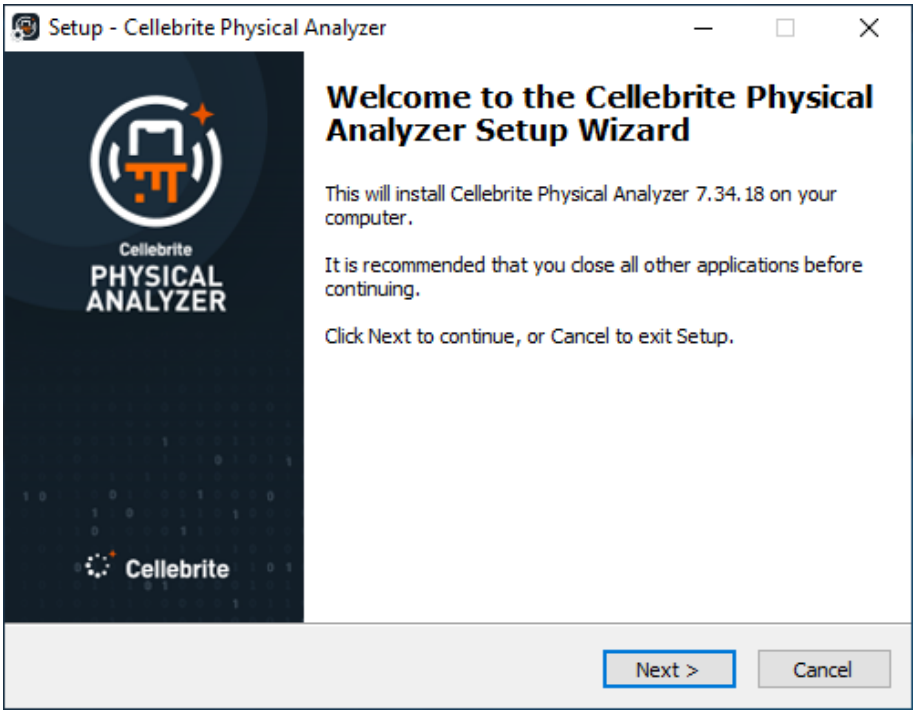
Before you begin, ensure that USB3 Host-to-Host cable is not attached to your computer.

PA setup includes an exe file and additional BIN files.

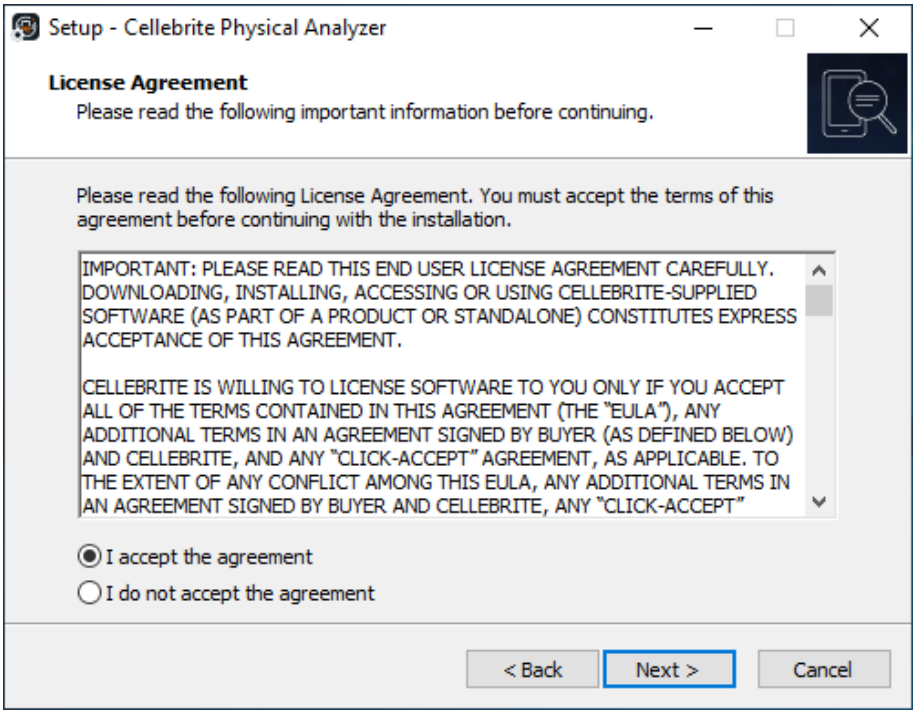
1. Double-click the Cellebrite_Physical_Analyzer_[version number].exe file.



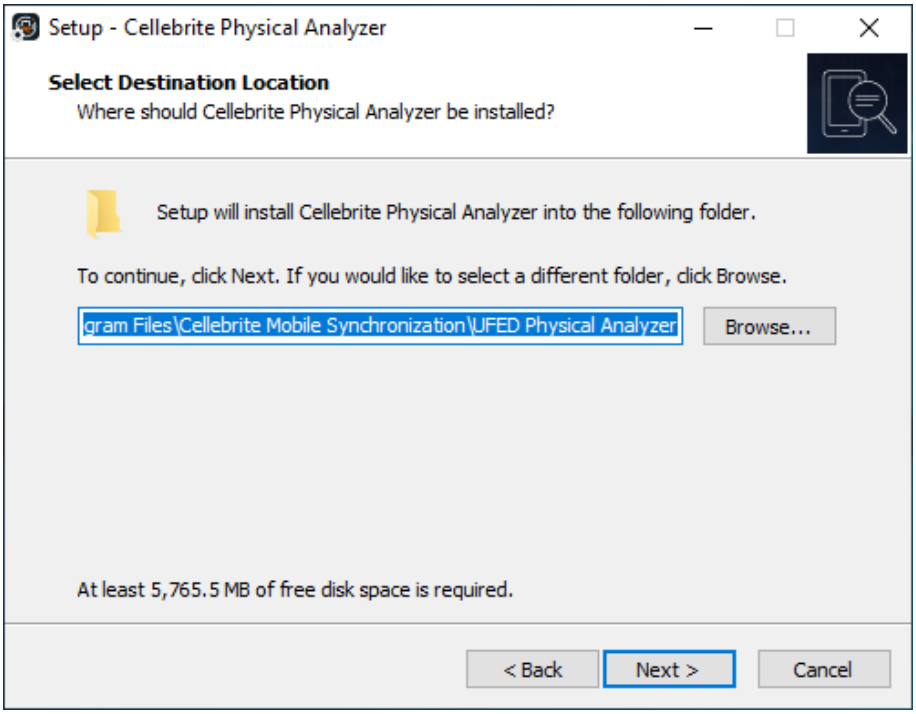
2. Select the desired language and click **OK** to continue. The following window appears.



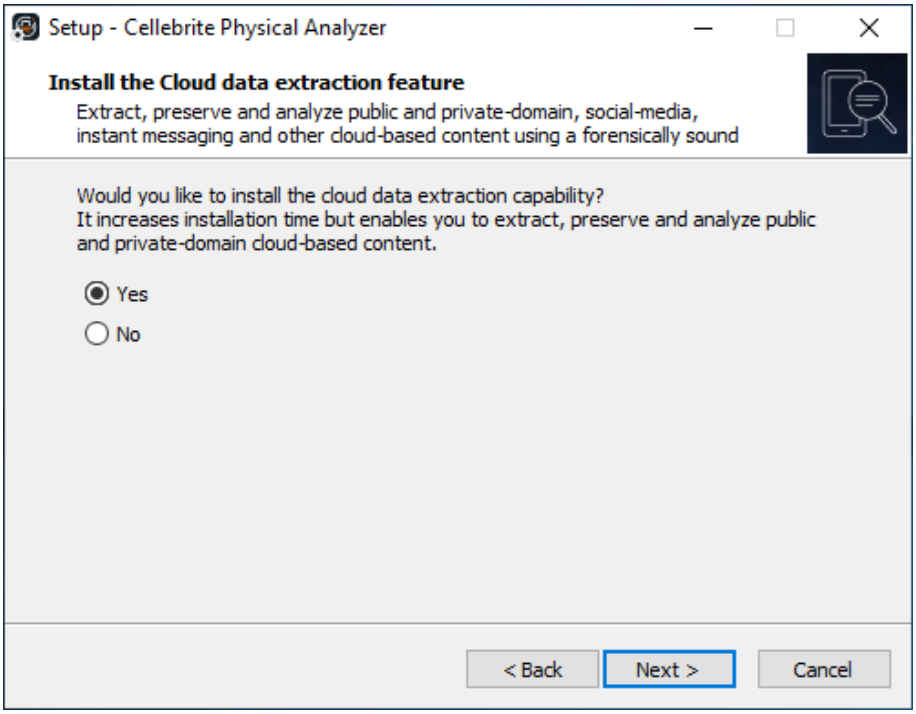
3. Click **Next**. The following window appears.



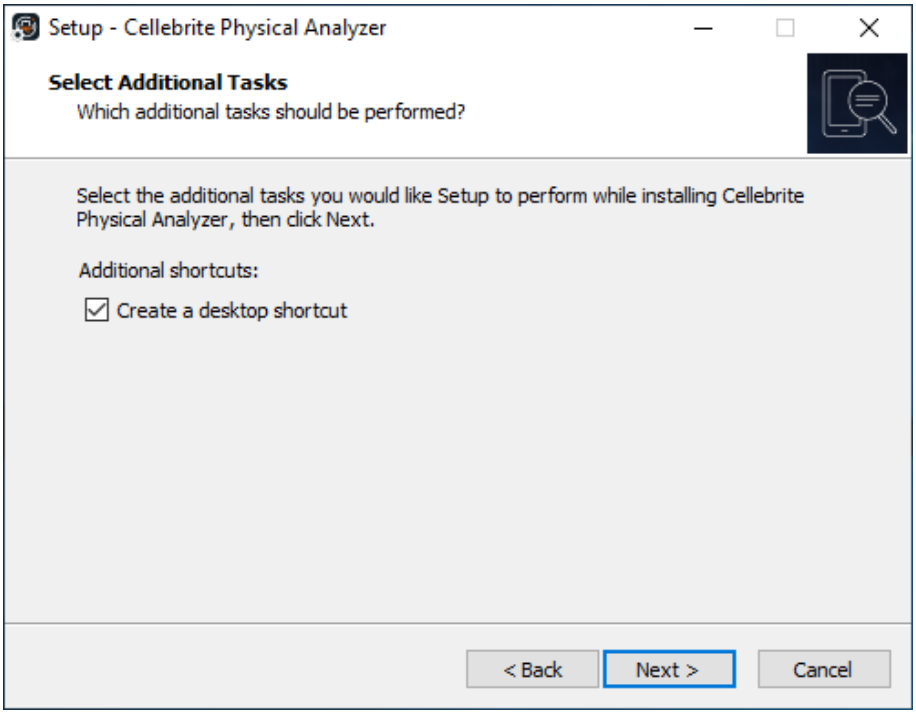
4. Read the agreement, select **I accept the agreement** and then click **Next**. The following window appears.



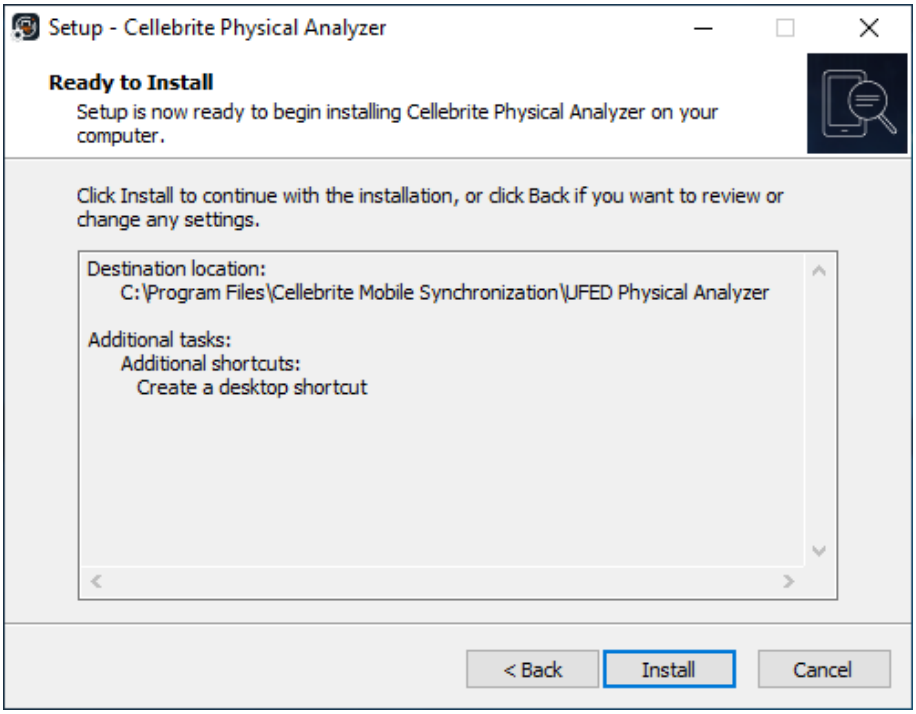
5. Click **Next** or if desired click **Browse** and set a different installation folder. The following window appears.



6. Select **Yes** to install the public data capability to enrich your examinations with public social media and cloud-based data. Internet access is required for this capability. If this capability is not required select **No**. The following window appears.

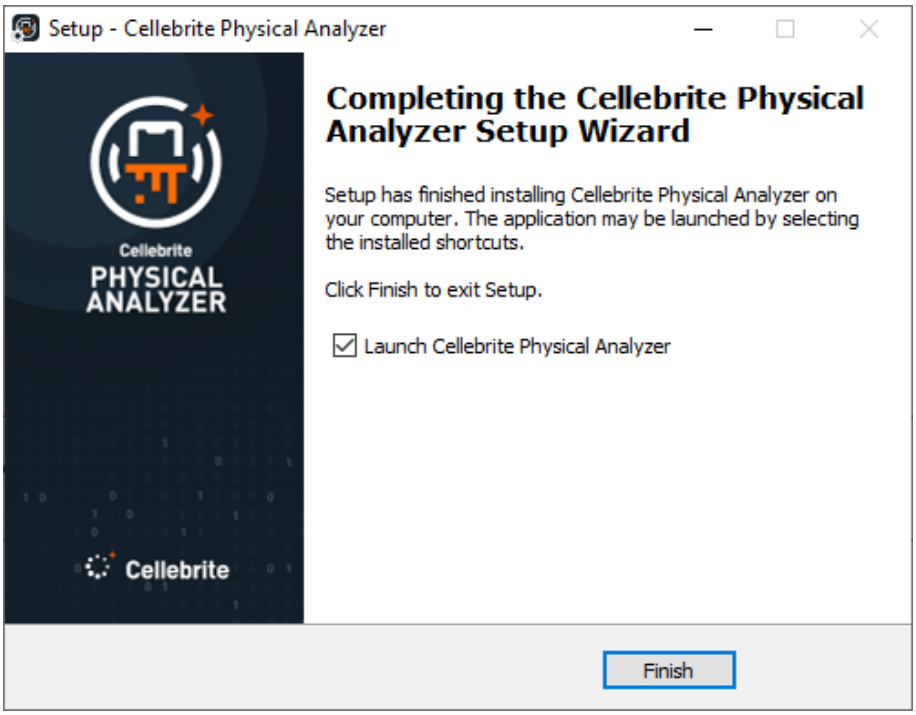


7. If you do not want a desktop icon, clear the **Create a desktop icon** check box, and then click **Next**. The following window appears.



8. Click **Install**. The installation begins.

> As part of the installation process, you may be prompted to download and install Microsoft .NET Framework. This is part of the installation and requires that your computer has Internet access.



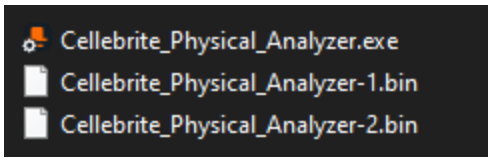
9. If you intend to activate the application using a hardware license key (dongle) provided by Cellebrite, select **Install Hasp Dongle Drivers**.

> You must have administrative rights to install the HASP dongle drivers.

10. To start the application at the end of the installation, select **Launch Physical Analyzer**.
11. Click **Finish**.

2.2.1. Silent installation

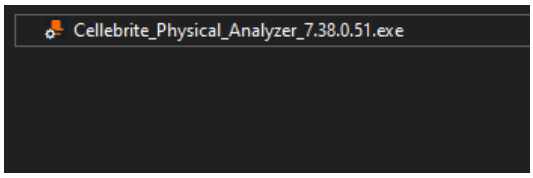
» For version 7.39 and newer installations, the .exe will include additional .bin files.



Running this silently can be done by using the following parameters:

"Cellebrite_Physical_Analyzer.exe" /verysilent /dir= (folderpath) /log=(folderpath)

» For version 7.38 and older installations, all of the files are consolidated into a single .exe file.



Running these executables silently can be done with these parameters:

"Cellebrite_Physical_Analyzer_7.38.0.51.exe" -sp /log=path /dir=path /verysilent

Other Parameters:

1. **Offline Maps:** The tileserver component of Physical Analyzer will be installed if it hasn't been installed yet and/or if nodejs isn't installed, the option to control the installation of it is not exposed in CLI.
2. **Cloud Extraction:** The parameter for skipping the Cloud extraction module is as follows:

   /CloudInstalled=1

Default installation log locations:

1. Windows temp folder:

   C:\Users\[localuser]\AppData\Local\Temp\Setup Log 2020-10-15.txt

2. There is also a log created in the directory where the .exe is being launched from:

   PA-setup.log

   The default log path can be changed by adding the /log= (folder path) as a parameter (as shown above).

Validating Installation:

1. The log file is approximately 9MB when complete.
2. It taked approximately 10 minutes for the installation to complete when performing an upgrade. It may be a few minutes longer for a fresh install since it is also installing the HASP Dongle drivers, offline maps tile server, etc.
3. For fresh installations, a restart of Windows is required at the end of the installation in order to ensure Dongle HASP drivers are full initialized. Restarts are not automatically triggered.

2.3. Activating the license

Activate Physical Analyzer in one of the following ways:

» Using a dongle license (on the facing page)
» Using a network dongle license (on page 27)

Check your kit to make sure which method you should use.

2.3.1. New version notification

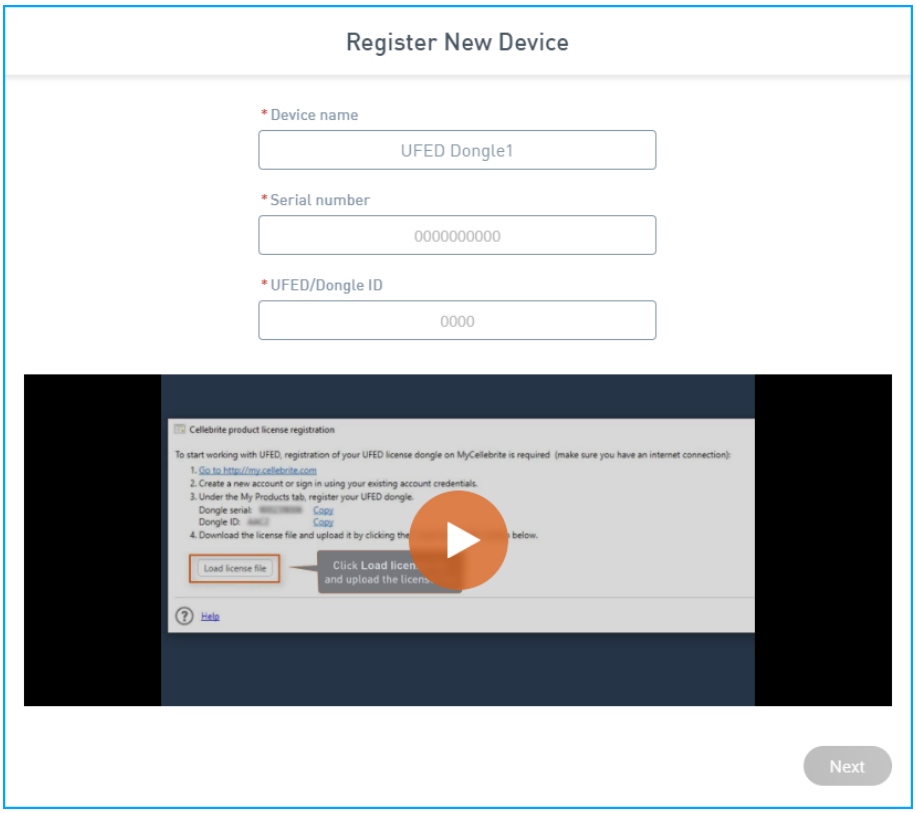
Cellebrite will inform you when a newer version of your software is available. If you are connected to the internet you will receive this notification when the new version is available. If you are not connected to the internet the notification will appear every 3 months.

2.3.2. Using a dongle license

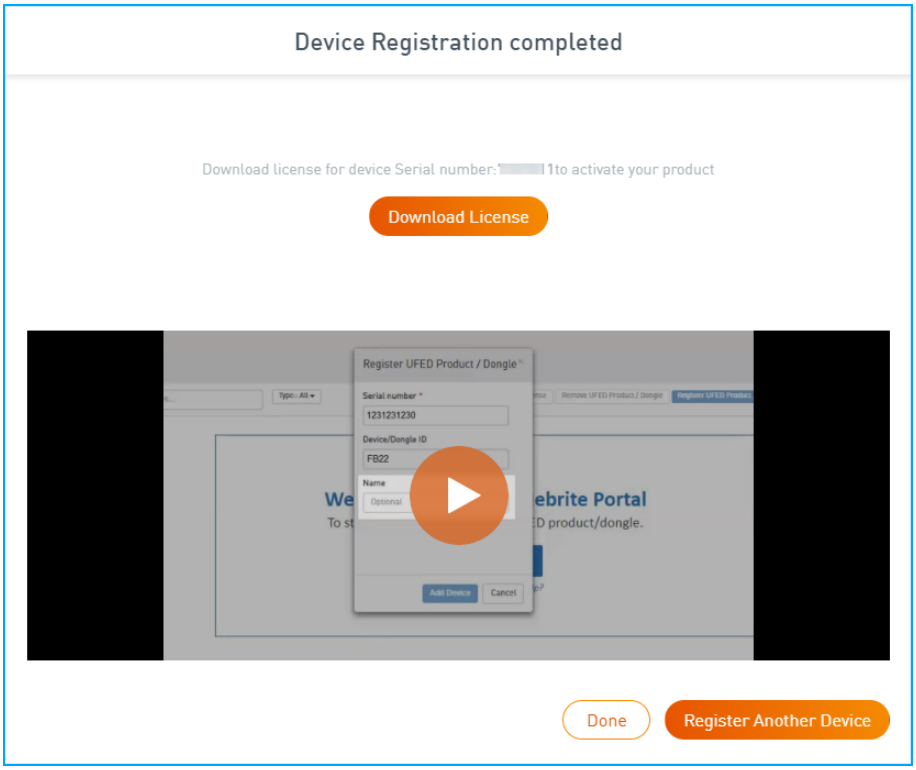
Use the Cellebrite UFED dongle provided with your Cellebrite UFED kit. The dongle contains licenses for all the applications purchased.

To use Physical Analyzer with a dongle:

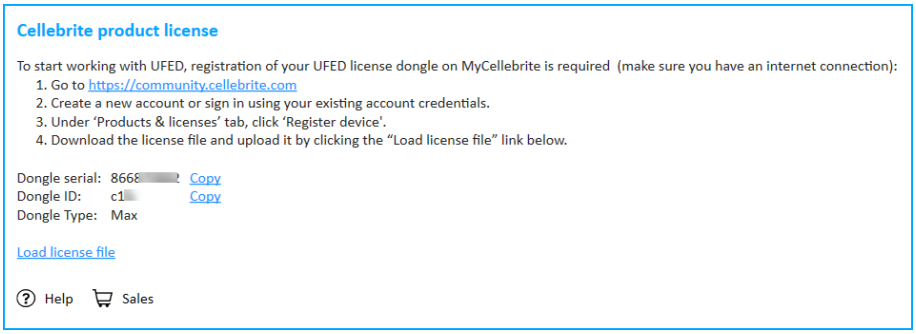
1. Go to community.cellebrite.com and log in with your credentials (or create an account).
2. Go to **Products & Licenses** > **Register Device** and enter a name for the device, the serial number and Dongle ID as displayed on the dongle.



3. Click **Next**. The following window appears.



4. Click **Download License** from the Device Registration Completed window to download the license key (or click **See licenses** in the Products tab and then from the menu on the right select **Download license**).
5. Download and install the Physical Analyzer application.
6. Start the Cellebrite UFED application and connect the dongle to a USB port on your computer. The following window appears.



7. In the Cellebrite product license window, click **Load license file** and upload the license key.

   Congratulations, your Physical Analyzer application is now ready!

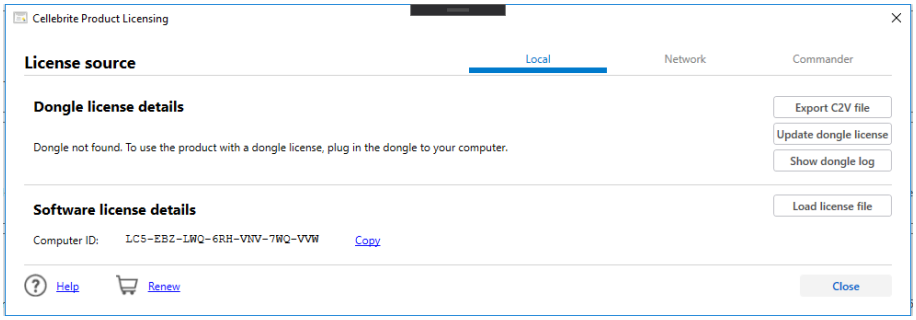
2.3.3. Using a network dongle license

The network dongle is connected to your organization's network and contains licenses for all the applications purchased.

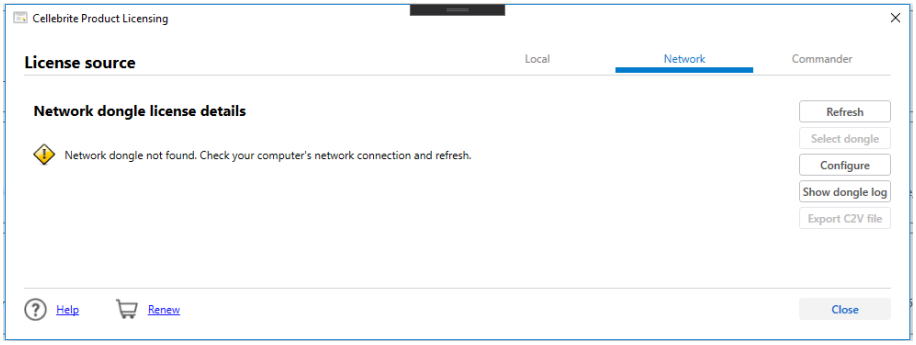
To use Cellebrite applications with a network dongle:

1. Start the application. If the network dongle is connected to the network, the application starts and the user can start working immediately.

   If the network dongle is not recognized, the Cellebrite Product Licensing window appears.



2. Click **Network**. The following window appears.



If a dongle was not found on the network – make sure that you have an Internet connection and that a dongle is connected to the network. Then click **Refresh** to search for a network dongle again.

By default, the network configuration is set to Broadcast. If required, you can manually connect to the network dongle. Click **Configure** to change the network configuration to Specific host. Enter the host name (or IP address).

If there is only one network dongle it will be selected automatically. If there are multiple network dongles, select the required dongle from the list and click **Apply**.

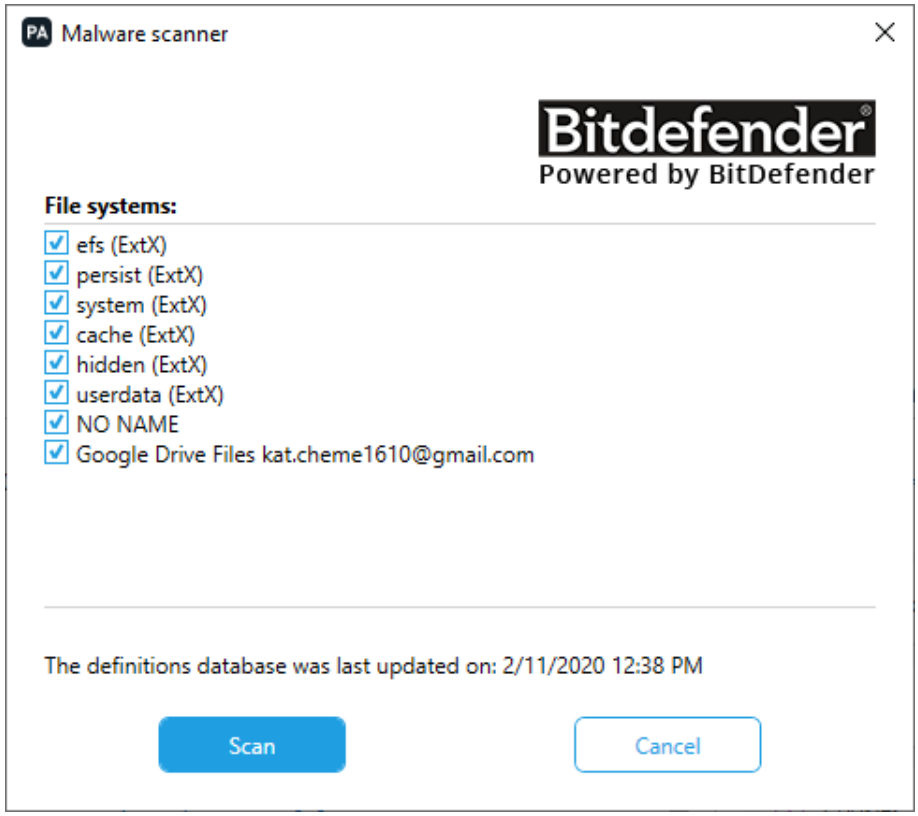
Congratulations, your application is now ready!

3. Scanning for malware

Run malware detection on your extraction to search for malware.

When you scan for malware, Physical Analyzer uses the last-used signature database. If this is the first time you are using the malware scanner, or if you want to update the database before you scan, follow the steps in Updating the signature database (online) (on the next page). If you are working on a computer without an internet connection, follow the steps in Updating the signature database from file (offline) (on page 31).

1. Select **Tools** > **Malware scanner** > **Scan Malware**. The following window appears.



2. Select the file system(s) that you want to scan, and click **Scan**.

   Physical Analyzer scans the project for malware. The results are displayed under the **Malware scanner** tree item.

3. Double-click the **Malware scanner** tree item to open a data display tab.

   The data shown includes the malware type and malware information, such as the name.

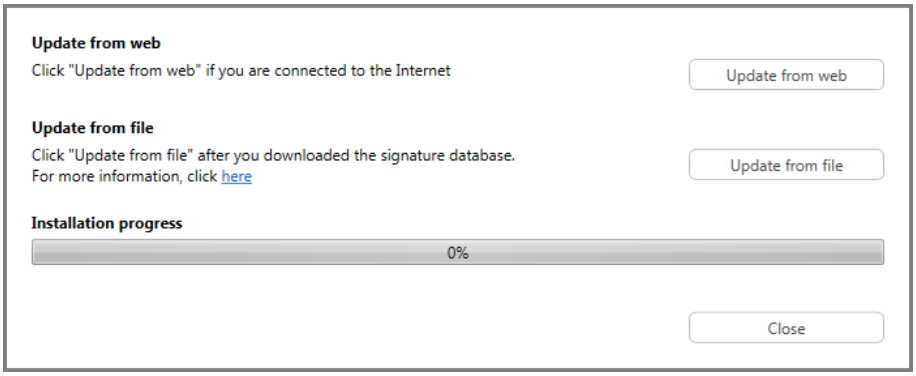
» To include the results in a report, select **Infected Files** in the **Report Dataset** area. For more information, see Generating a report (on page 257).

3.1. Updating the signature database (online)

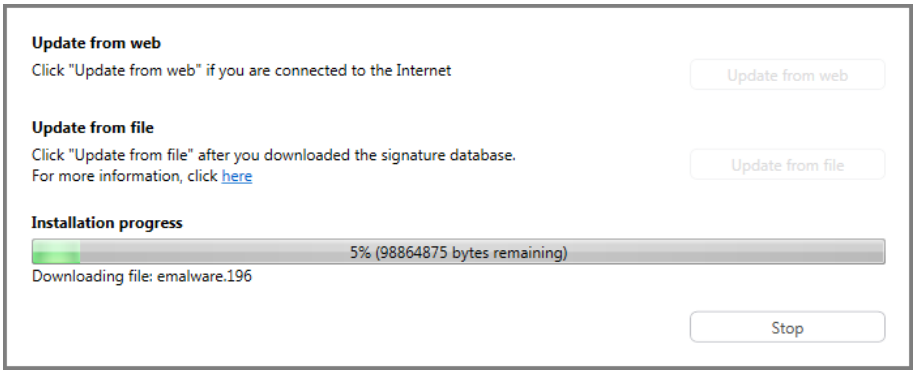
Update the signature database before the first time you use the malware scanner in order to populate the database, and thereafter in order to keep the signature database up to date.

> Once the signature database is populated, you can run the malware scanner using the existing database. It is strongly recommended that you update the signature database on a regular basis in order to keep it current.

1. In the **Tools** menu, select **Malware scanner** > **Update signature database**. The following window appears.



2. Click **Update from web**. The database is populated.



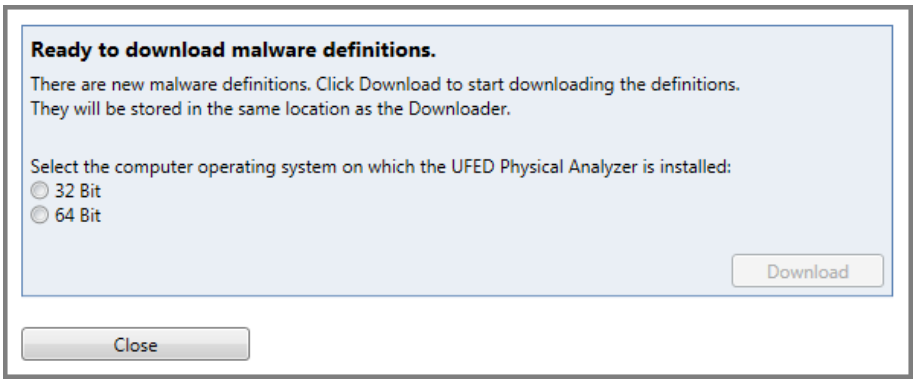
3. Upon completion, click **Close**. You can now scan the project for malware.

3.2. Updating the signature database from file (offline)

Update the signature database from file when you are working on a computer that does not have an internet connection.

> Once the signature database is populated, you can run the malware scanner using the existing database. It is strongly recommended that you update the signature database on a regular basis in order to keep it current.

1. In Windows Explorer, in the main Physical Analyzer directory, copy the **BitDefenderUpdater** directory to an external storage device.
2. Transfer the **BitDefenderUpdater** directory to a computer that has internet connection without proxy settings.
3. In the **BitDefenderUpdater** directory, double-click **Malware Definitions Downloader.exe**.



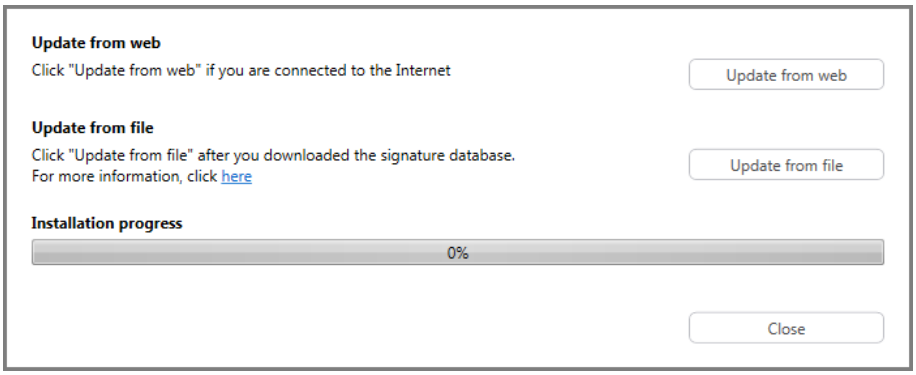
4. Select the computer operating system of the computer on which Physical Analyzer is installed.
5. Click **Download**. The following window appears.

6. Click **Open containing folder**.
7. Copy the **definitions.msd** file to an external storage device, and transfer it to the computer on which Physical Analyzer is installed.

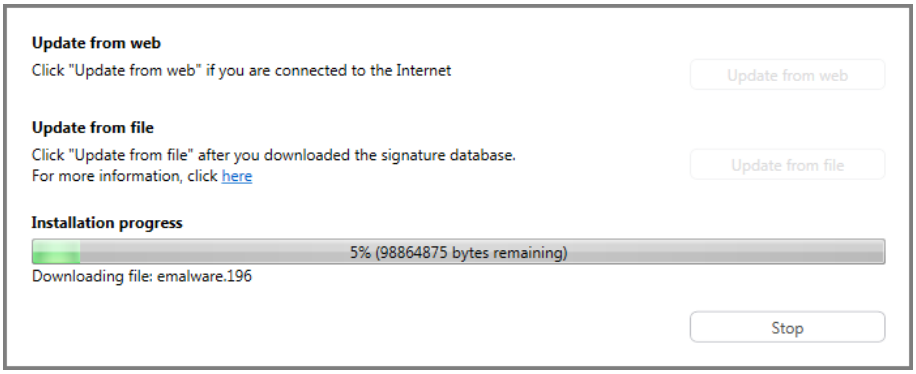
8. Click **Close** to close the Malware Definitions Downloader.

> To streamline your workflow and save time, it is recommended that you always use the same computer to download the **definitions.msd** file. When you download the **definitions.msd** file to this computer in the future, the Malware Definitions Downloader updates the file instead of downloading the entire file. Make sure that you do not delete the **definitions.msd** file from this computer.

9. In Physical Analyzer, select **Tools** > **Malware scanner** > **Update signature database**. The following window appears.



10. Click **Update from file**. The Open file window appears.
11. Browse to the malware definitions database file (*.msd), and click **Open**.
12. Click **Start**. The database is populated.



13. Upon completion, click **Close**. You can now scan the project for malware.

4. Getting started

Physical Analyzer provides powerful decoding and analysis tools for the extracted device data, and simplifies the task of navigating through the device's data structures. Physical Analyzer assists you in the complex tasks of intelligence gathering, investigative research, and providing legal evidence in the form of reports.

The application is designed to utilize the memory extracted by UFED and present the device's Hex extraction, file system and analyzed data in a clear and concise way, allowing investigators to use powerful search tools to reveal relevant information.

As a completing step, the application enables you to generate reports of your findings in various file formats, such as HTML, PDF, Excel (*.xlsx), and XML.

To learn more about performing extractions on cloud based data sources see, Cloud extractions (on page 208).

4.1. Starting Physical Analyzer

To start Physical Analyzer, do one of the following:

- Double-click the **Physical Analyzer** desktop shortcut.
- Select **Start > Programs > Cellebrite Mobile Synchronization > Physical Analyzer**.

For an overview of the workspace, see Orientation to the workspace (on page 81).

4.2. Opening an extraction for analysis

Physical Analyzer can open files created by the UFED device, XML files created by the Physical Analyzer, UFDR files, UFD files, and URP files. In Advanced mode, it can open image and other files. For more information, see Open (Advanced) (on page 42).

If the device data was extracted to a removable drive, connect the USB flash drive or SD card containing the extracted data to your PC.

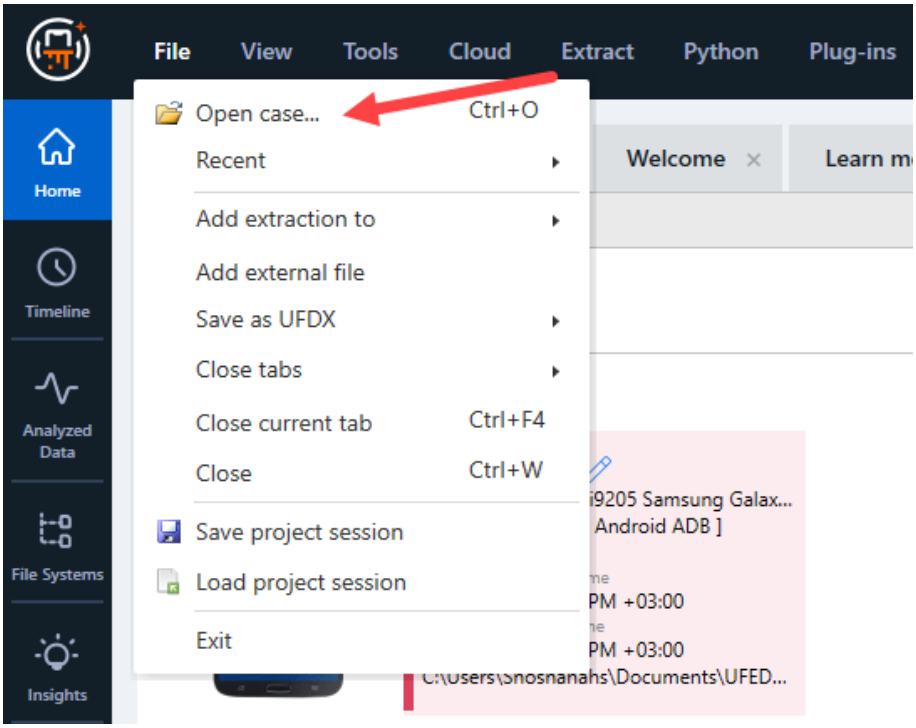
For faster processing, copy the extraction folder from the removable media to the PC.

For information on opening an extraction using the case wizard, see Using the case wizard (on the next page).

4.3. Using the case wizard

A case wizard leads you through the steps to start your investigation in Physical Analyzer, and load all related evidence for decoding and examination.

The case wizard enables you to create a new case, with relevant case information and upload multiple extractions (or other evidence). You can also merge extractions and examine hash sets, carve locations, and activate Watch lists. You can eliminate the time-consuming tasks of reviewing and correlating multiple extractions with the power of Text and Media analytics.



> 32 GB of RAM is recommended to use both Physical Analyzer and Cellebrite Pathfinder on the same computer. The minimum is 16 GB of RAM.

> A GPU is recommended.

The case wizard steps are as follows:

» Loading evidence (on page 36)
» Examination tools (on page 69)

4.3.1. Starting the case wizard

To start the case wizard:

1. From the application menu, select **File** > **Open case**.

   Or do one of the following:

   - In the **Welcome** tab, click on a recent file.
   - Drag-and-drop the UFD file into Physical Analyzer.

4.3.2. Loading evidence

In this step, you can select multiple extractions to decode and examine in a single step. All extractions will be merged under a single project or device.

> This first step is mandatory. You can skip the other steps by clicking **Examine data** to initiate the decoding process.

Loading extractions is described next.

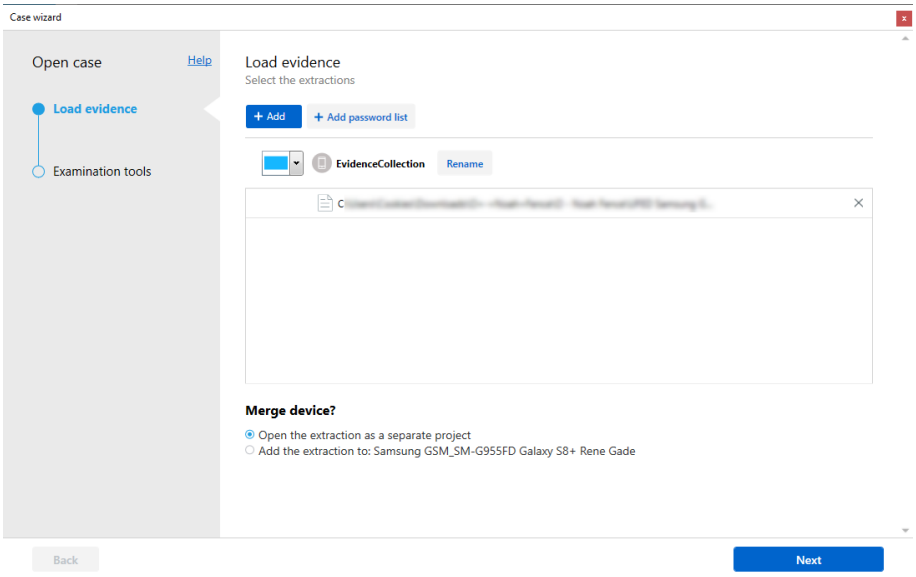
For information on loading other types of evidence, see the following topics:

Warrant returns (on page 40)

GrayKey (on page 41)

Open (Advanced) (on page 42)

Common sources (on page 56)



This window provides the following functionality:

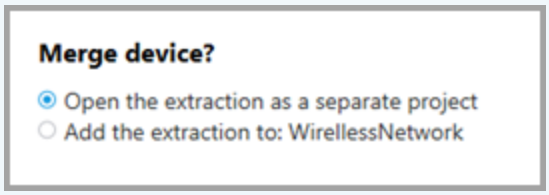
+ Add	Add an extraction.
+ Add password list	Upload a password list (a dictionary file of all known passwords) before decoding. See Using password lists: (on page 38)

	Select a color to represent the person.
	Rename the device.
×	Remove extractions.

To load evidence:

1. Select **Add** > **Load extraction** and select the extraction to add. The following file formats are supported:
   - UFDX collection (*.ufdx)
   - UFED dump (*.ufd)
   - Binary files (*.bin). Raw binary files or any Hex extraction generated by another application using the advanced opening feature. See Open (Advanced) (on page 42).
   - Nokia PM (*.pm)
   - BlackBerry backup file (*.ipd, *.bbb)
   - Sony Ericsson GDFS (*.gdfs, *.bin)
   - TomTom CFG (*.cfg)
   - UFED report (*.xml)
   - E01 (*.e01)
   - UFED Report Package (*.ufdr)
   - Report Manager (*.urp, *.ucp) - UFED Report Pack/UFED Content Pack reports created by Report Manager
   - Cellebrite Responder package (*.zip)
2. Browse to the location of the extracted device data folder and open it.
3. Click **Next** to go to the Examination tools (on page 69) step.

If an extraction is already open, you can select to merge this extraction with the exciting person or open the extraction as a separate project.



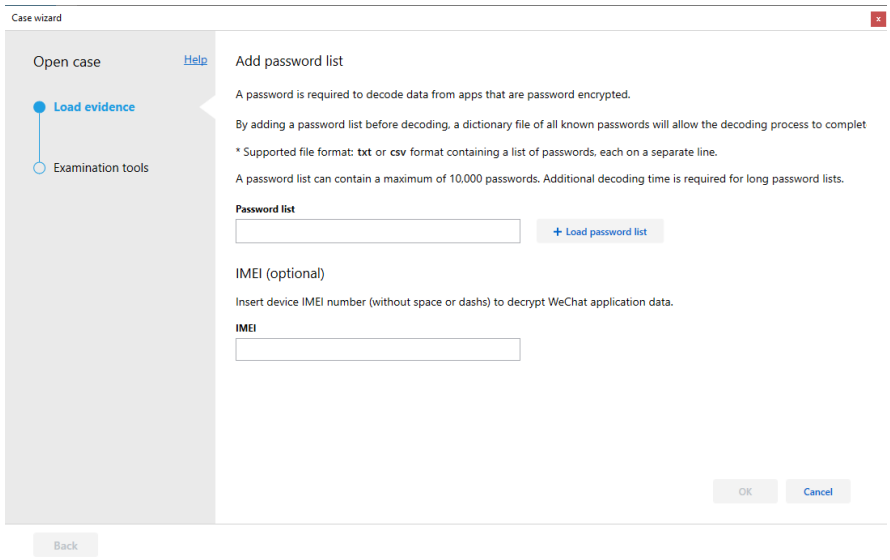
Using password lists:

Some encrypted apps and sources may require a password to enable decryption/decoding. In these cases, you are required to enter the correct password to successfully decode the data.

By adding a password list (a dictionary file of all known passwords), you can set the passwords while creating a case to prevent interruptions while the data is being decoded.

1. In the case wizard, click **Add password list.**
2. Click **Load password list** to add a .txt or .csv file containing the list of passwords.
3. Enter the IMEI number to decrypt WeChat application data (optional).

4. Click **Ok**.


Case wizard
Open case
Help
Load evidence
Examination tools
Add password list
A password is required to decode data from apps that are password encrypted.
By adding a password list before decoding, a dictionary file of all known passwords will allow the decoding process to complet
* Supported file format: txt or csv format containing a list of passwords, each on a separate line.
A password list can contain a maximum of 10,000 passwords. Additional decoding time is required for long password lists.
Password list
+ Load password list
IMEI (optional)
Insert device IMEI number (without space or dashs) to decrypt WeChat application data.
IMEI
OK
Cancel
Back

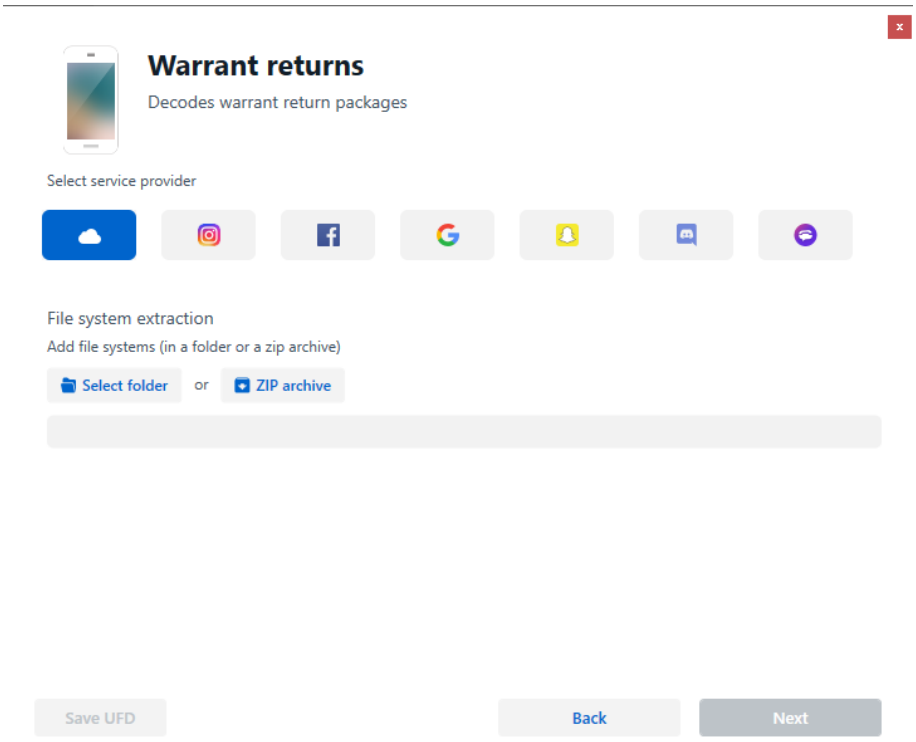
4.3.2.1. Warrant returns

Decodes warrant return packages from the following service providers:

- **Apple iCloud:** Decodes data from iCloud backups received from Apple as evidence.
- **Instagram**: Decodes Instagram Warrant return files.
- **Facebook:** Decodes Facebook Warrant return files.
- **Google:** Decodes Google Warrant return files.
- **Snapchat:**Decodes Snapchat Warrant return files.
- **Discord**: Decodes Discord Warrant return files.
- **TextNow**: Decodes TextNow warrant return files.

To decode warrant returns:

1. Select **Add** > **Warrant returns**. The following window appears.



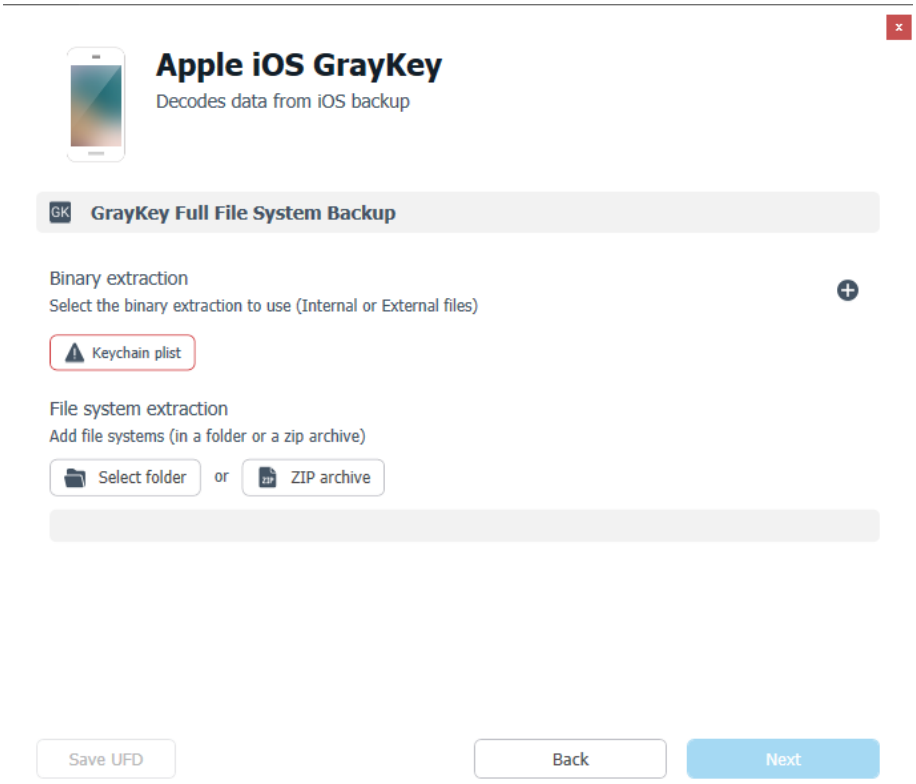
2. Select the service provider.
3. Select the file system extraction (folder or zip file). For more information, see Adding a file system extraction (on page 49).
4. (Optional). Click **Save UFD** to save a .ufd file for this project. If you create a UFD file, you will not have to go through this process again in the future to open this particular case.
5. Click **Next**.

4.3.2.2. GrayKey

Decodes iOS data from full file system extractions.

To decode Apple iOS GrayKey extractions:

1. Select **Add** > **GrayKey**. The following window appears.



2. Select the keychain plist (optional).
3. Select the file system extraction (folder or zip file). For more information, see Adding a file system extraction (on page 49).

> GrayKey extractions include both full file system (binary image) and the external keychain plist file (not part of the folder or zip file). In a single session, you can decode both the GrayKey image and the keychain plist files.

4. (Optional). Click **Save UFD** to save a .ufd file for this project. If you create a UFD file, you will not have to go through this process again in the future to open this particular case.
5. Click **Next**.

4.3.2.3. Open (Advanced)

The Open (Advanced) feature enables you to specify the device data extraction and decoding options.

Select from two main project opening methods:

- **Select a UFED extraction** - Enables you to specify how to decode a UFED extraction file (*.ufd). See Advanced opening of a UFED extraction file (below)
- **Start without a .ufd file** - Enables you to start to decode a physical extraction or a file system that was not generated by a UFED unit. See Advanced opening of a non-UFED extraction file (on page 49)

> This feature is available with Physical Analyzer only.

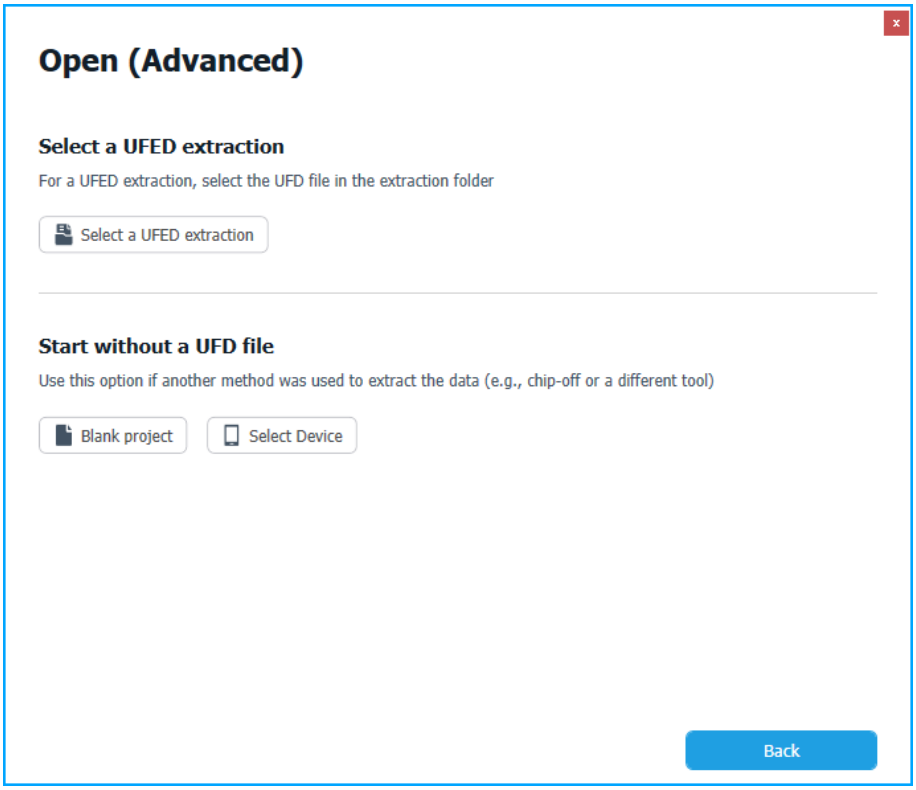
4.3.2.3.1. Advanced opening of a UFED extraction file

The standard open process activates a decoding process set according to the device and manufacturer information logged in the *.ufd file.

Using the **Open advanced** method enables you to skip the standard Open process, and specify a custom parsing process, or specify how to parse unknown devices.

To create a new project from UFED extracted data using Open (advanced):

1. Select **Add** > **Open (advanced)**. Thefollowing window appears, enabling you to set the process of decoding the extracted data for your new project.



2. Click Select a UFED extraction.
3. In the Open dialog, select the *.ufd file to be processed and click OK. The following window appears.

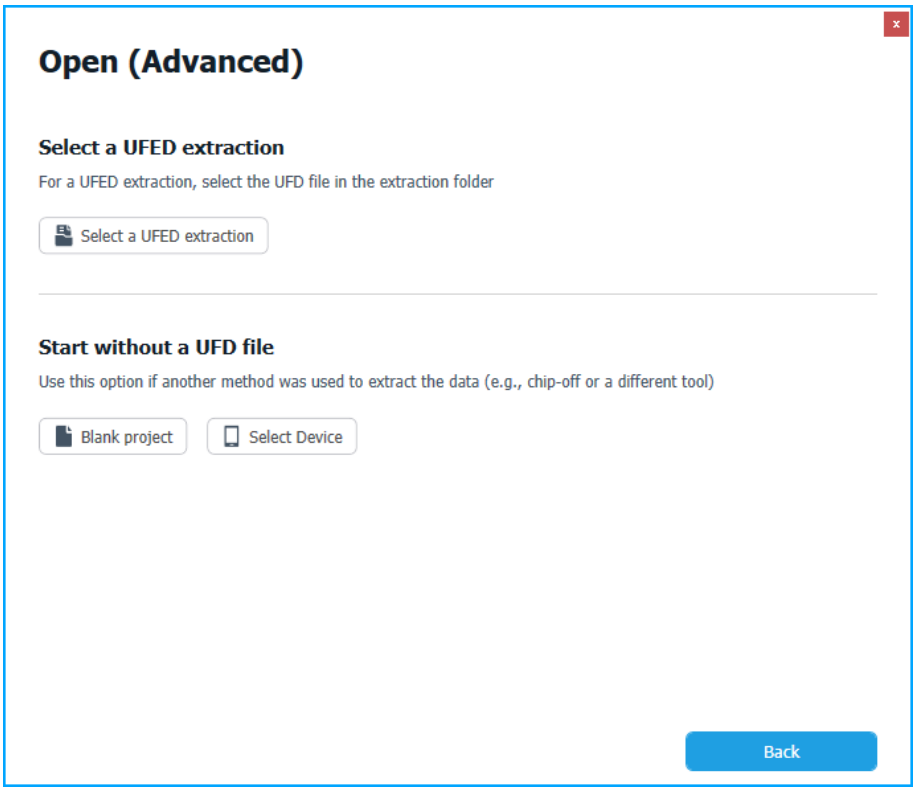
If required, you can click to switch the selected device, switch chain or customize the chain. For more information, see Changing the decoding chain (on the facing page).

4. Select the file system extraction (folder or zip file). For more information, see Adding a file system extraction (on page 49).
5. (Optional). Click **Save UFD** to save a .ufd file for this project. If you create a UFD file, you will not have to go through this process again in the future to open this particular case.
6. Click **Next**.

Specifying a different device

You can specify an entirely different decoding process for the extraction by replacing the selected device.

1. From the Open (advanced) dialog, click **Switch Device**. The following window appears.



2. From the **Select Device** list, select the desired device.
3. To filter the displayed devices, do one of the following:
   - Click on device manufacturer in the list of manufacturers on the left pane
   - Enter the device manufacturer or model in the **Quick Filter** field to filter the displayed devices
4. Click **Next** to return to the Advanced Customization panel.

Changing the decoding chain

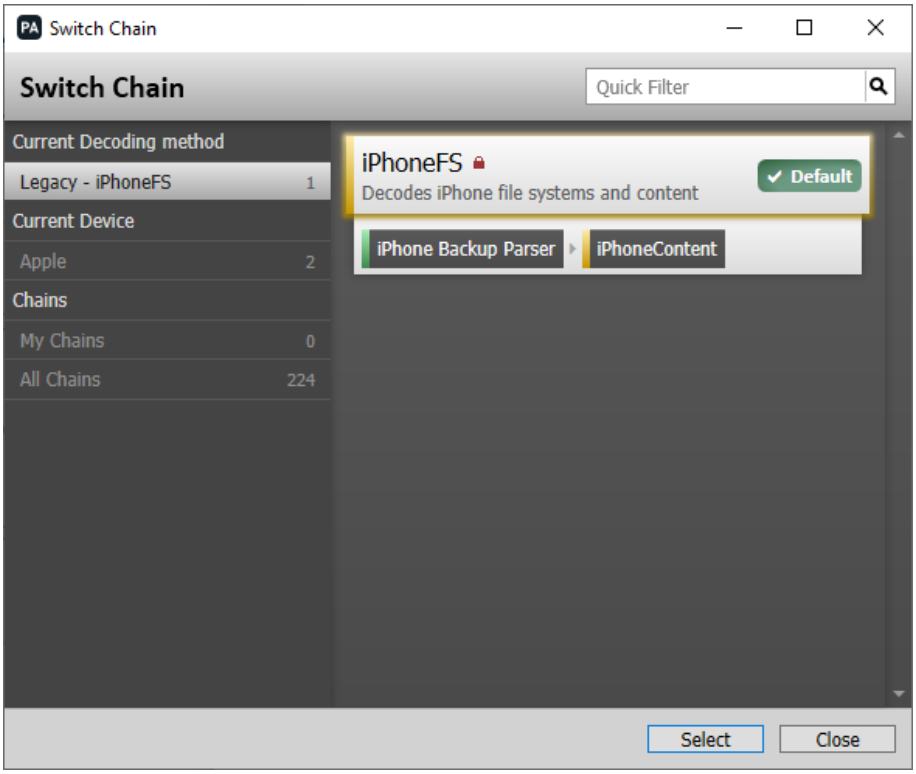
A chain is a set of plug-ins grouped together in a certain order, which is used to decode the extracted data. Each device in the supported devices list of the application has a predefined decoding chain assigned to it.

> Beside plug-ins, a chain can also include other chains, a simpler way to use a predefined set of plug-ins within another chain.

For more information about decoding chains and plug-ins, see Advanced decoding (on page 404) and Plug-ins (on page 416).

To select a different chain:

1. In the Open (advanced) dialog, click **Switch Chain** ( ). The Switch Chain dialog opens and displays the default chain assigned to the device.



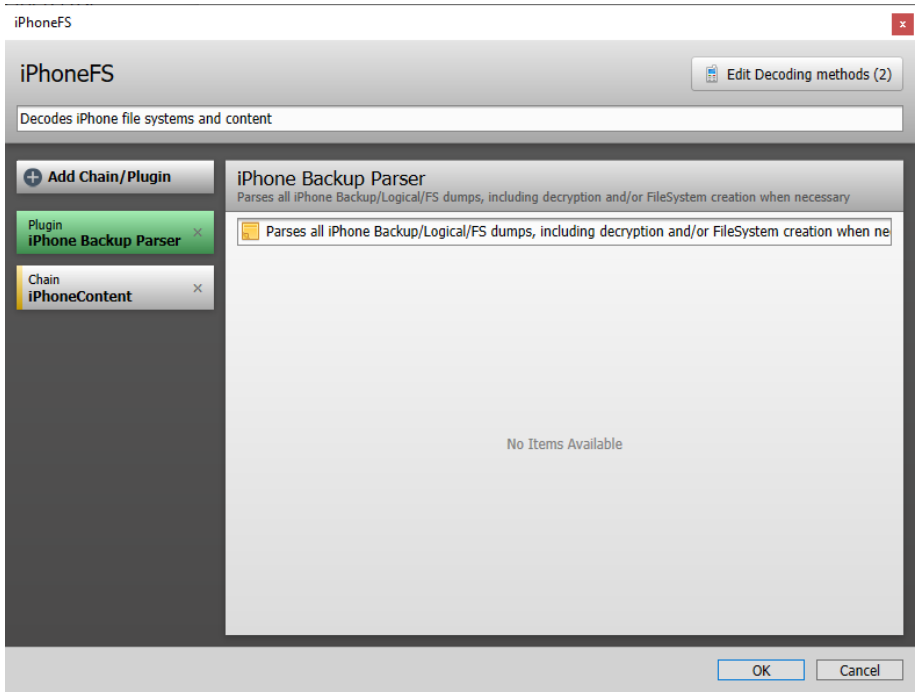
> A device can have several assigned chains, but only one of them can be set as the default chain.

2. From the chains list, select the desired chain in one of the following ways:
   - Select the manufacturer name under the **Current Device** section to display the chains assigned to devices of the same manufacturer.
   - Under the **Chains** section of the list:
   - Select **My Chains** to select from the list of custom chins you constructed.
   - Select **All Chains** to select from the list of all predefined device chains.
   - Use the Quick Filter field to filter the displayed list items.
3. Select the relevant chain, and click **Select** to return to the Advanced Customization panel.

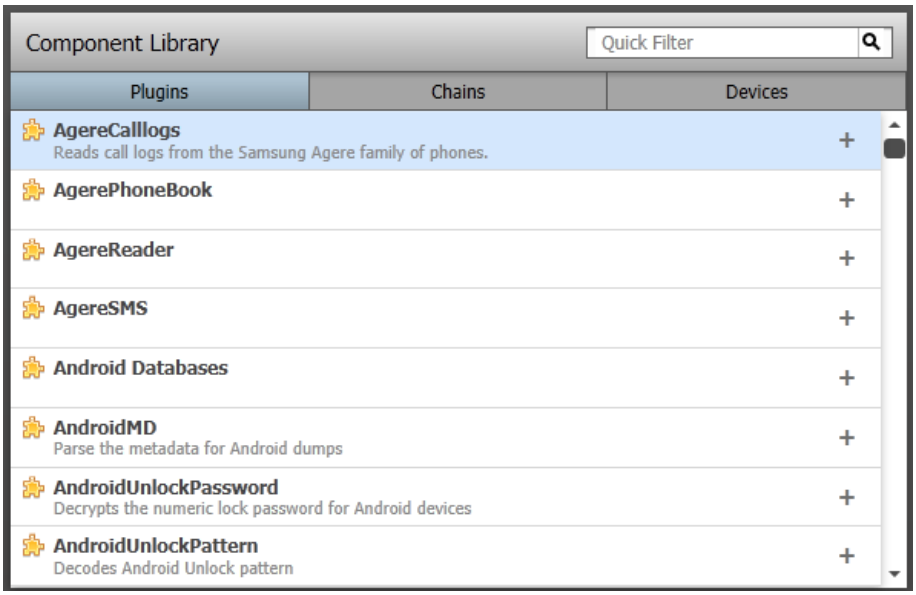
   The default chain is replaced by the selected chain.

To edit the current chain:

1. Click **Edit** ( ). The chain structure dialog of the current chain opens and displays the chain.



2. To add a component to the chain:
   a. Click **Add Chain/Plugin**.
   b. From the **Component Library**, select one of the following:



   - **Device**: The entire chain of a specific device.
   - **Chain**: A specific predefined chain.
   - **Plugin**: A specific plug-in.

> Items selected under both **Device** and **Chain** are added to the chain as a **Chain component**.

3. Click **+** to add the component.
4. To remove a component from the chain list, click the x at the right of the component item, then click **Yes** to approve.
5. Click **OK** to return to the Advanced Customization panel. The default chain is replaced by the customized chain.

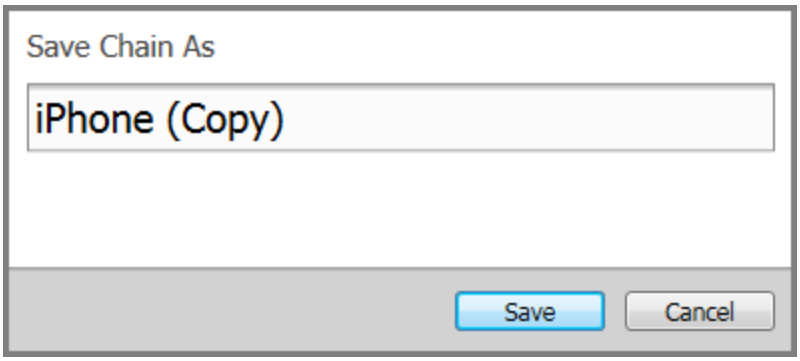
To save a customized chain:

After you customize a chain, you can save the changes made to the chain for future use using the **Save As** or **Save** buttons in the **Selected Chain** section.

> The **Save** button is available only for customizations for unlocked user-defined chains saved in **My Chains**. For more information about user defined chains, see Managing chains (on page 404).

1. Click **Save** to replace the user-defined chain with the current one or **Save As** to save the current chain as a new chain.

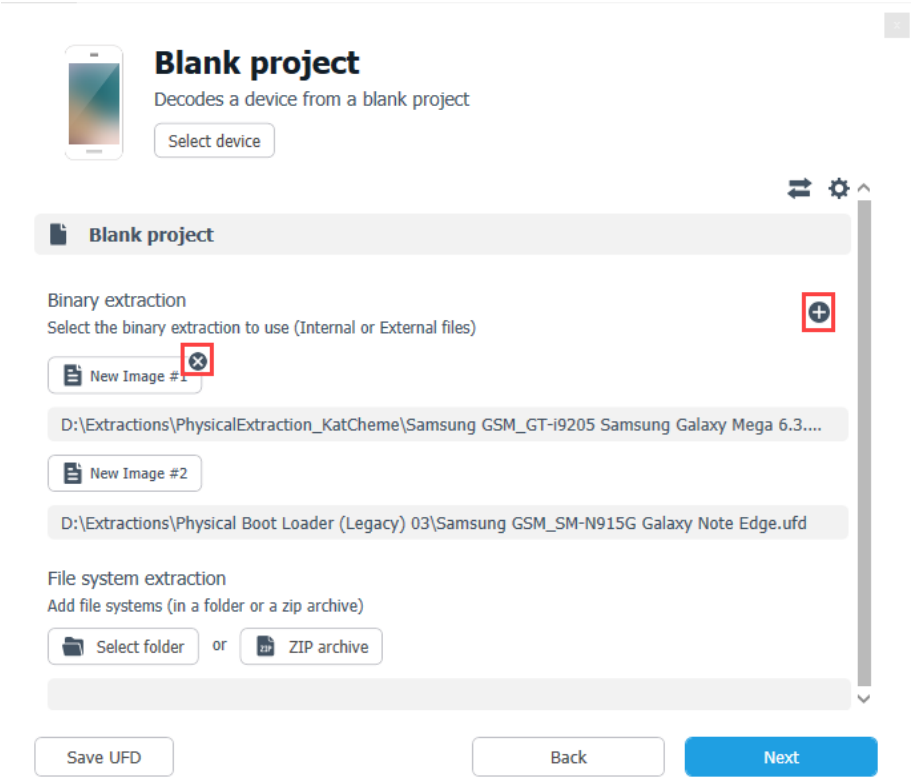
2. If you clicked **Save As**, enter a name for the new chain and click **Save**.



The new chain is added to the **My Chains** list of customized chains of the application, and the saved chain appears as the **Selected Chain**.

Adding a binary dump

You can add additional binary dump (extraction or image) files received from different sources in Open (advanced).



» Click ⊕ to add an extraction. Each binary extraction you add is shown in the window.

» To remove an extraction, click the ⊗ that appears when you position the mouse over it.

Adding a file system extraction

You can add a file system extraction to the project received either as a ZIP archive or as a folder containing the file system extraction files.

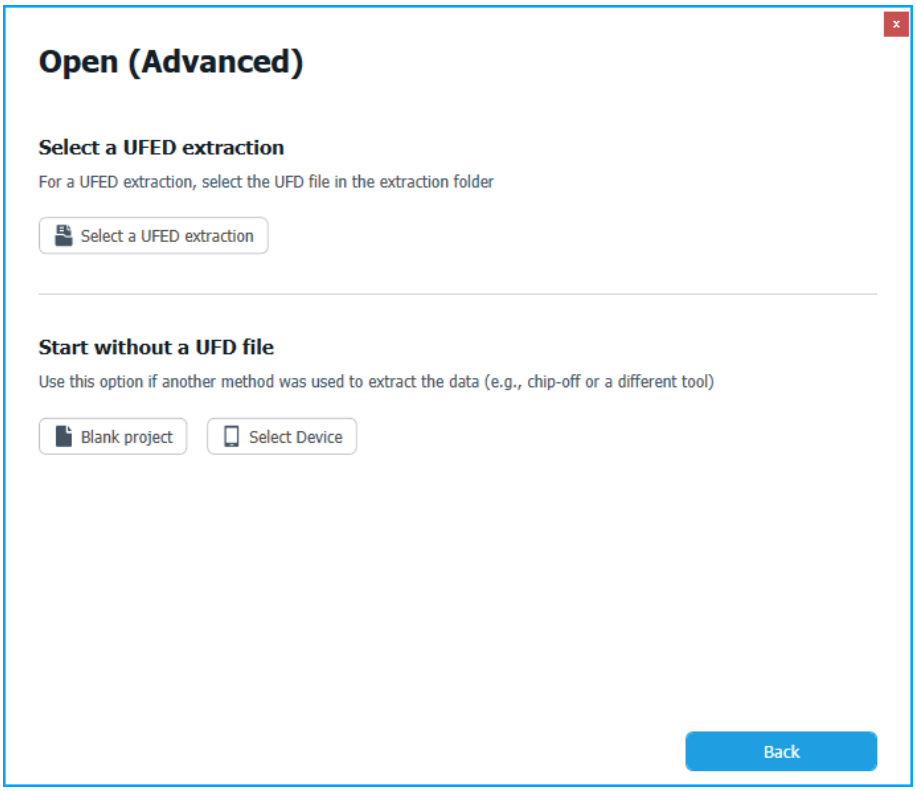
» To add a file system extraction, click either **Zip Archive (ZIP, TAR or DAR)** or **Folder,** and select the archive or folder you wish to add.

> You can add one file system extraction only. Trying to add more than one removes the previously added file system extraction, regardless of whether it's a zip archive or folder.

4.3.2.3.2. Advanced opening of a non-UFED extraction file

When you receive binary or file system extractions that were not generated by a UFED unit, or you don't have the *.ufd file that accompanies them, you can use the Open (advanced) feature to define how to decode them for the new project.

1. Select **Add** > **Open (advanced)**. The Open (advanced) dialog appears, enabling you to set the process of decoding the extracted data for your new project. The following window appears.

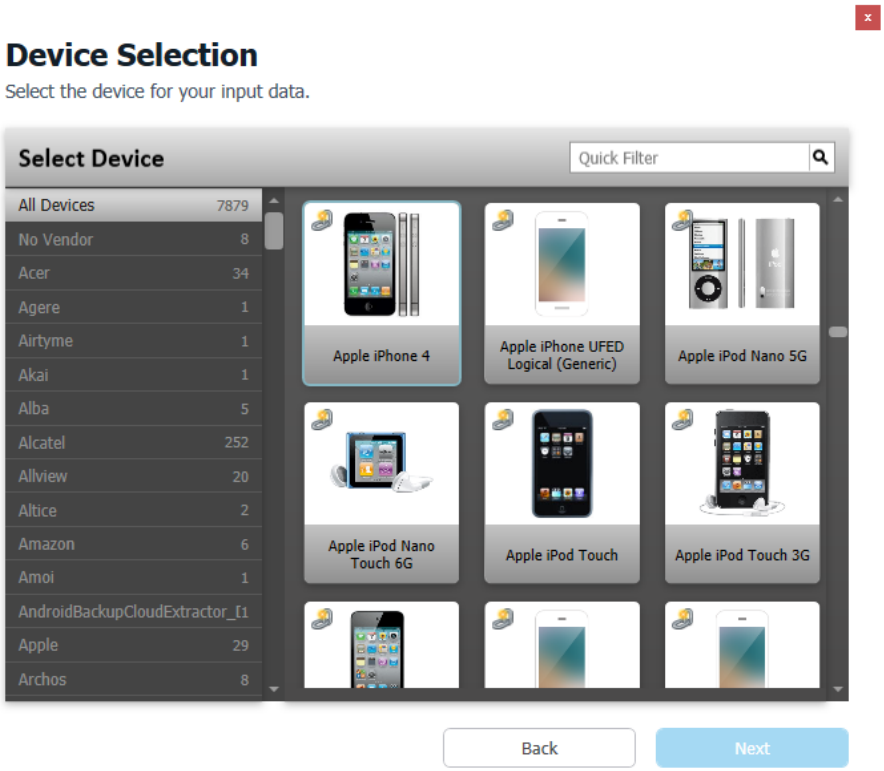


2. The **Start without a UFD file** option provides you with two starting points for your new project:
   - **Blank Project:** Provides you with an empty **Advanced Customization** panel to set your process parameters and data. This option is useful when you have no information about the device and/or manufacturer, and would like to construct a custom decoding process. See Starting from a blank project (on the facing page).
   - **Select Device:** Select the specific device definition to use to decode the data extraction. This option is useful when the device manufacturer and model are known to you. See Starting with device selection (below).

Starting with device selection

Create a new project for data extraction based on a known device.

1. In the Open (Advanced) window, click **Switch Device**.
2. From the **Select Device** list, select the desired device.



3. Use the list of manufacturers on the left to filter the displayed devices by manufacturer, and the **Quick Filter** field to filter the displayed devices by any string.
4. Click **Next**.

   The Advanced Customization panel displays the name and default decoding chain of the selected device.

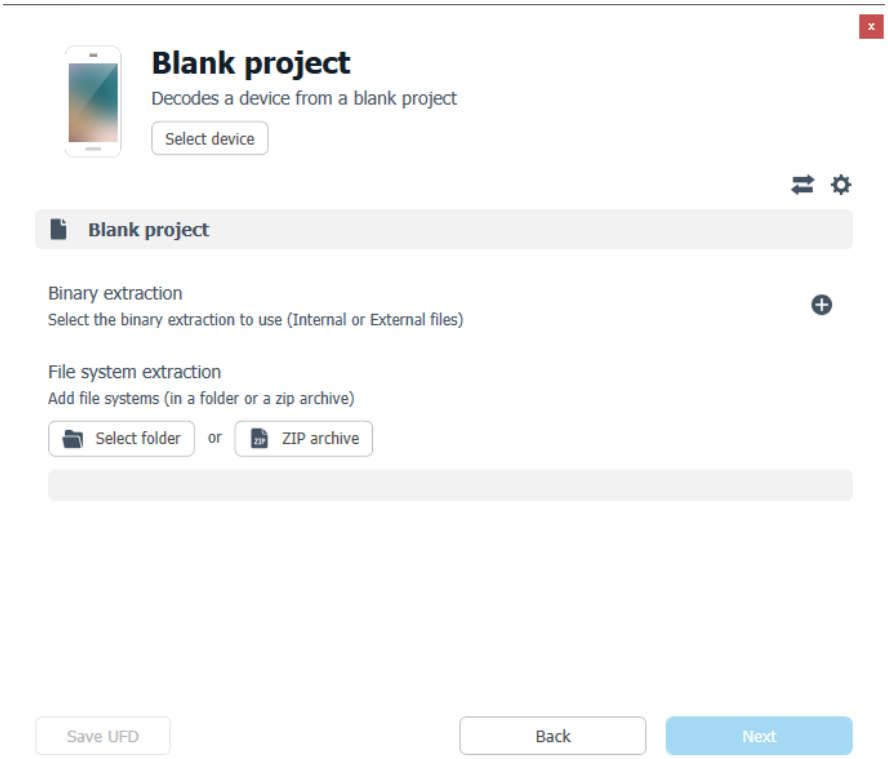
   - To select a different device, see Specifying a different device (on page 44).
   - To select a different parsing chain, see Changing the decoding chain (on page 45).

» To customize the parsing chain, see Changing the decoding chain (on page 45).
» To add a file system extraction, see Adding a file system extraction (on page 49).

5. (Optional). Click **Save UFD** to save a .ufd file for this project. If you create a UFD file, you will not have to go through this process again in the future to open this particular case.
6. Click **Finish**.

Starting from a blank project

1. In the Open (Advanced) window, click **Blank project**. The following window appears.



2. To select a device, see Specifying a different device (on page 44).
3. To select a parsing chain, see Changing the decoding chain (on page 45).
4. To customize the parsing chain, see Changing the decoding chain (on page 45).
5. To add binary extractions, see Adding a binary dump (on page 48).
6. To add a file system extraction, see Adding a file system extraction (on page 49).
7. (Optional). Click **Save UFD** to save a .ufd file for this project. If you create a UFD file, you will not have to go through this process again in the future to open this particular case.
8. Click **Finish**.

4.3.2.3.3. JTAG extractions

JTAG (Joint Test Action Group) is an advanced method of data extraction that requires a forensic examiner to connect to the test access ports of the device to obtain a full physical image. This enables the examiner to unlock and gain access to the raw data stored on the memory chip.

JTAG is non-destructive and offers the opportunity to access data from devices that have been altered or damaged in some, where data ports are unavailable (or disconnected), or it is otherwise impossible to unlock the device using other forensic tools.

Physical Analyzer automates the JTAG decoding process and saves you time in that you no longer need to manually decode the large volume of raw data found in JTAG extractions.

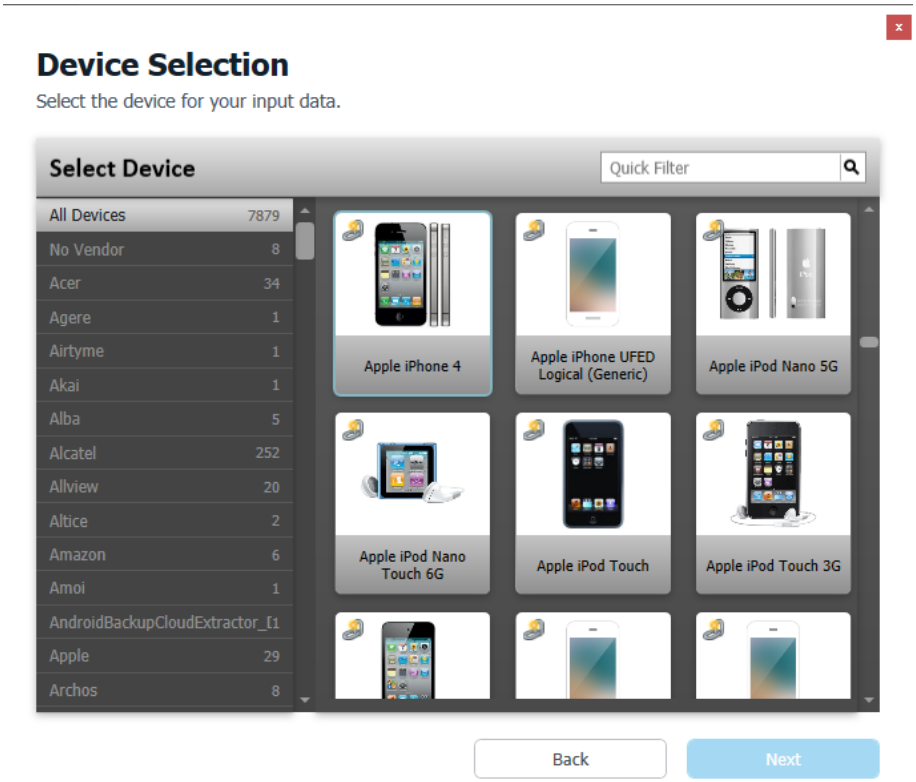
For an updated list of devices that support JTAG extractions, refer to the UFED Phone Detective Mobile App or the UFED Supported Devices document in MyCellebrite.

Once you have the physical memory that was acquired with this method, you can load it into the Physical Analyzer for decoding. When loading the appropriate UFED JTAG chain, you will receive all the data, as if it was a regular extraction.

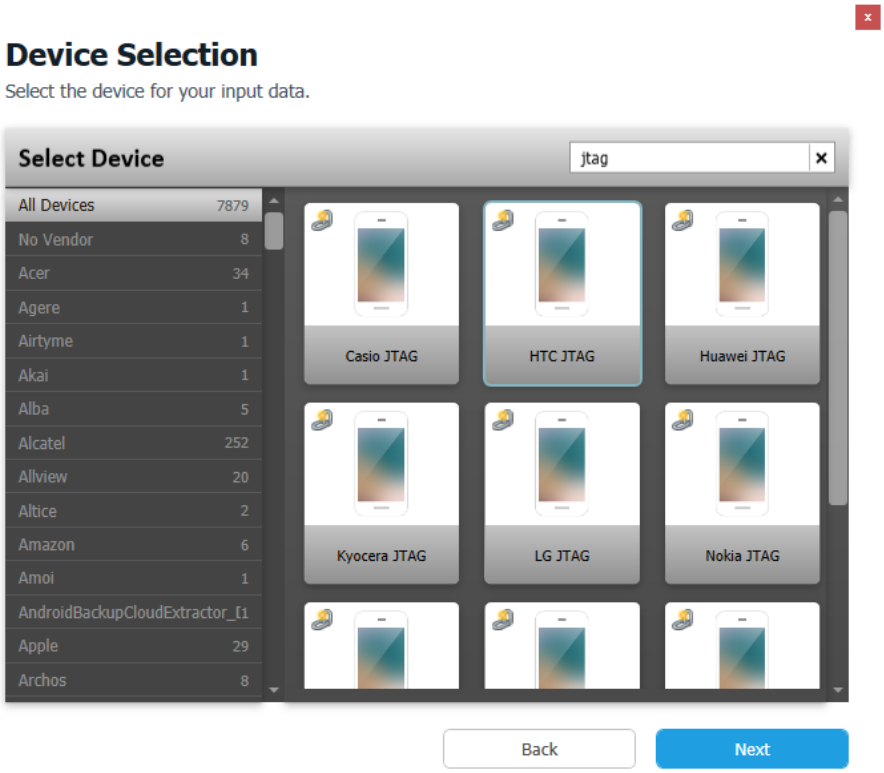
The main difference between a JTAG extraction and a UFED extraction are the locations of "spares" inside the extraction. Spares are the technical term for metadata of blocks inside the extraction. They can be located in several locations inside the extraction. In regular extractions, they are located at the end of each block. In JTAG extractions they are located at the end of the extraction.

To decode the data extraction using JTAG:

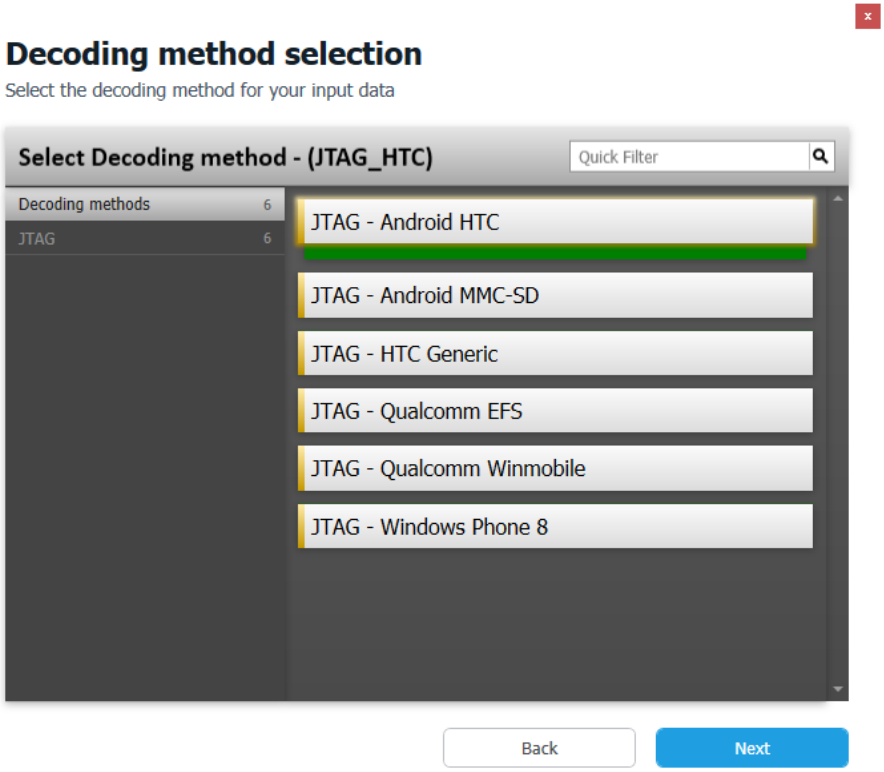
1. In the Open (advanced) window, click **Select Device**.
2. To filter the displayed devices, enter the device manufacturer or model in the **Quick Filter** field, or click on device manufacturer in the list of manufacturers on the left pane.



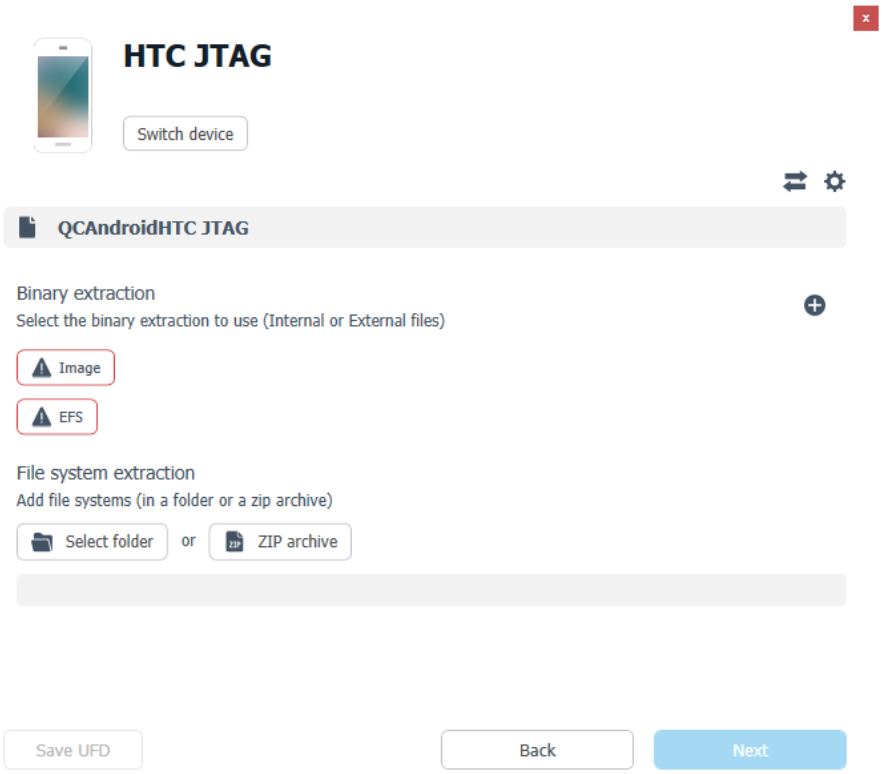
If JTAG is not supported for the required device you can enter “jtag” In the Quick Filter field to select a generic JTAG device.



3. Select the required device and click **Next**. The following window appears.



4. Select the decoding method and click **Next**. The available methods change from device to device. The following window appears.



5. Click to add a binary extraction. Each binary extraction you add is shown.
6. Click **Next**.

4.3.2.3.4. Saving a .ufd file

At any point of setting the Open (advanced) parameters, you can click **Save UFD** to save a *.ufd file that logs the selected binary extractions and device information for future use. The next time you need to decode that case, you can just open the UFD file.

4.3.2.4. Common sources

Common decoding plug-ins:

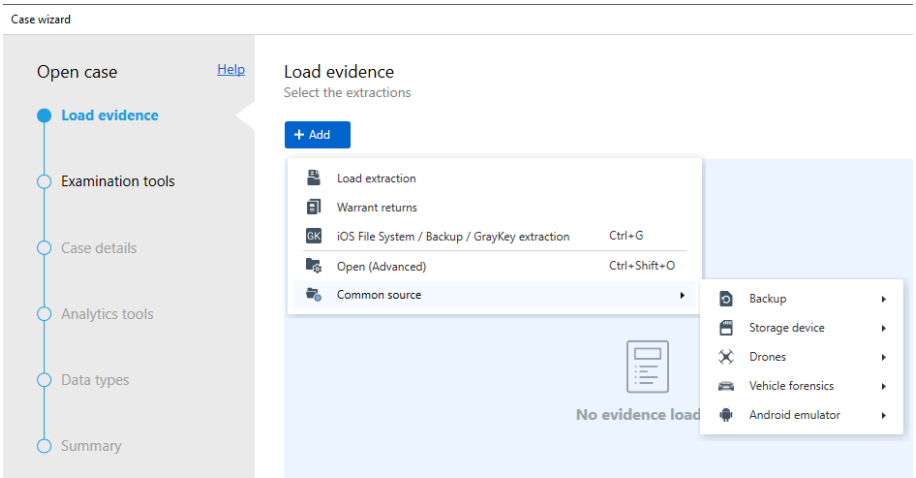
Backup (on the facing page)

Storage device (on page 62)

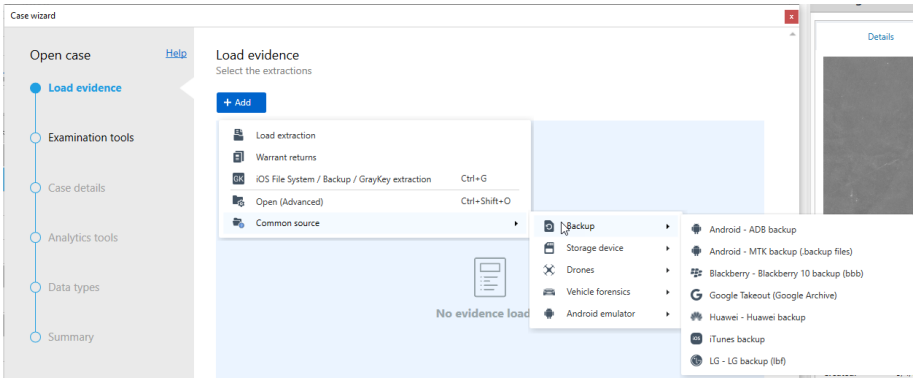
Drones (on page 63)

Vehicle forensics (on page 64)

Android emulator (on page 65)

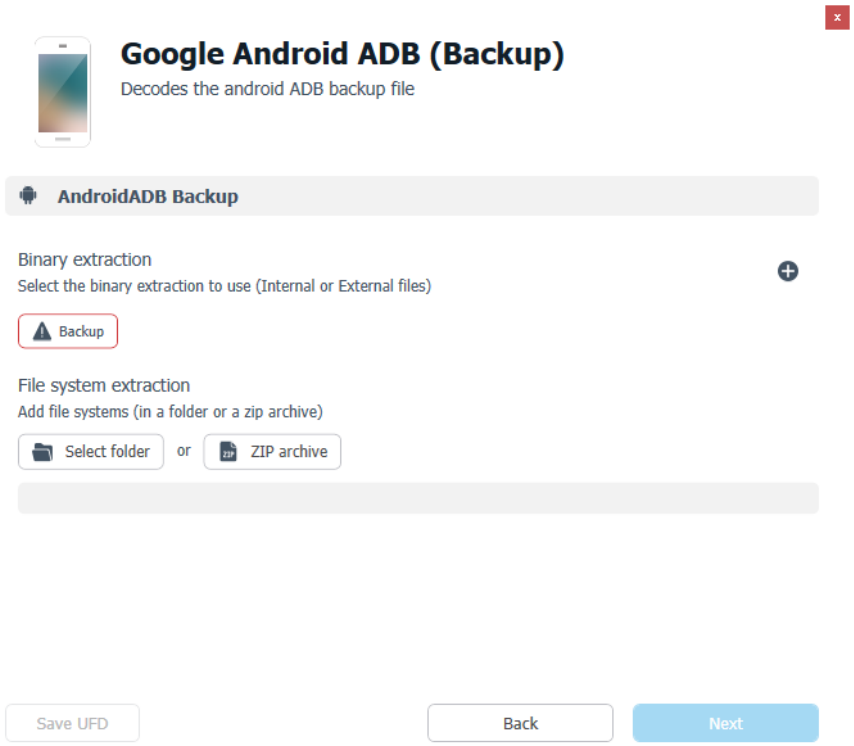


4.3.2.4.1. Backup



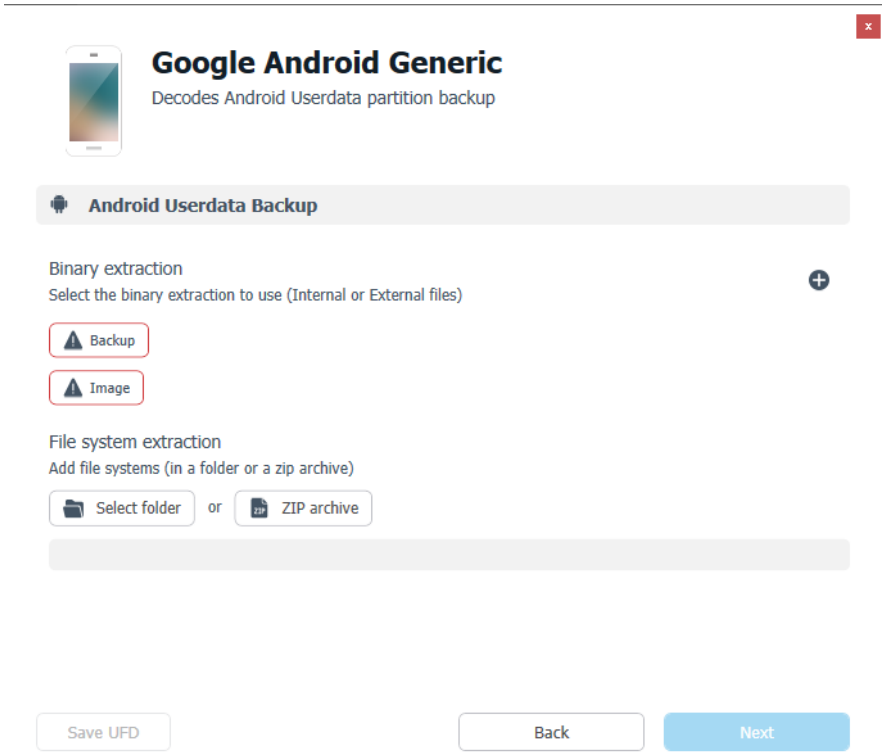
» Select **Common source** > **Backup** > **Android - ADB backup**

Decodes Android ADB backup files.



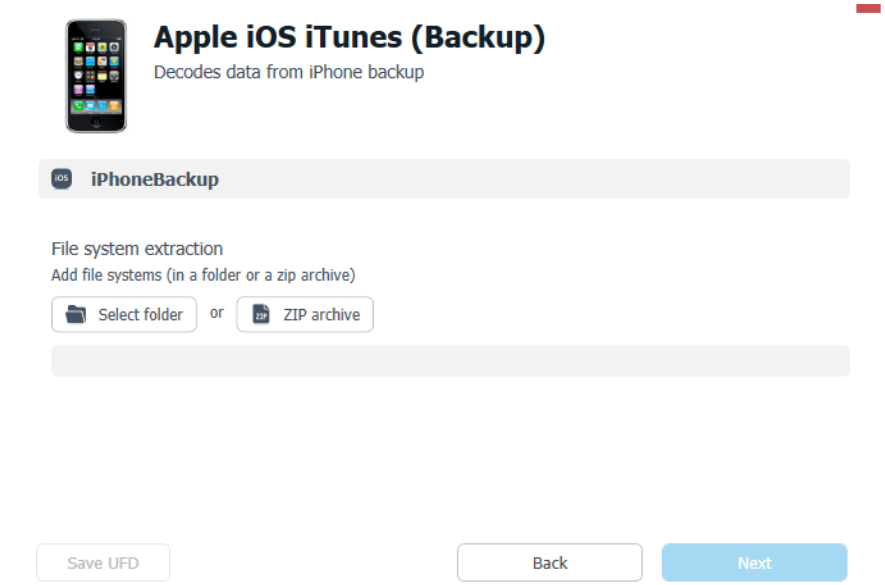
» Select **Common source** > **Backup** > **Android - MTK backup (.backup files)**

Decodes Android MTK backup files.



» Select **Common source** > **Backup** > **iTunes backup**

Decodes data from iPhone backups.

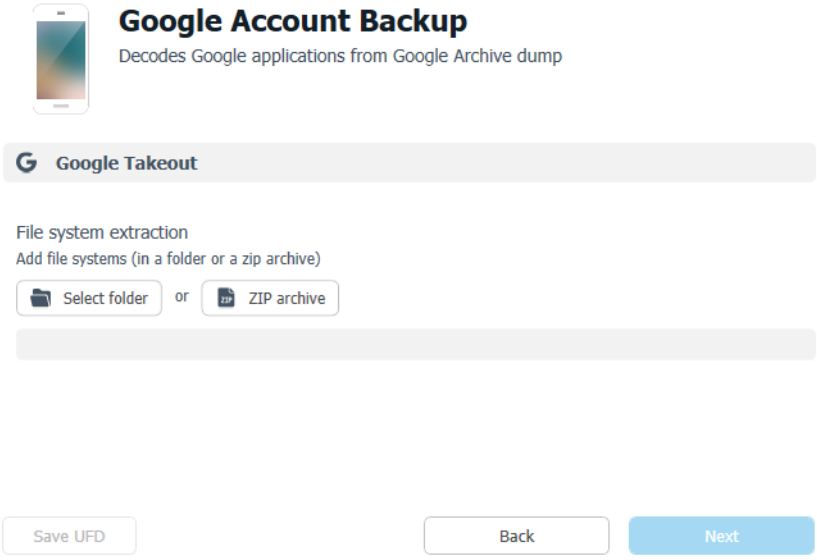


» Select **Common source** > **Backup** > **BlackBerry - BlackBerry 10 backup (bbb)**

Decodes BlackBerry10 bbb backup files.

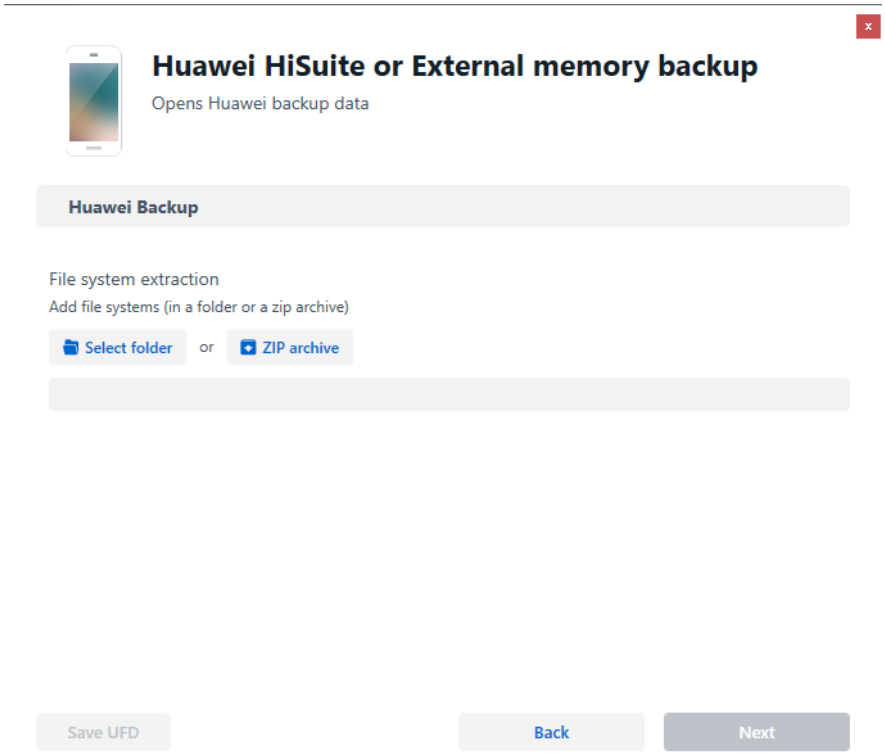
» Select **Common source** > **Backup** > **Google Takeout (Google Archive)**

Decodes Google applications from Google Takeout.



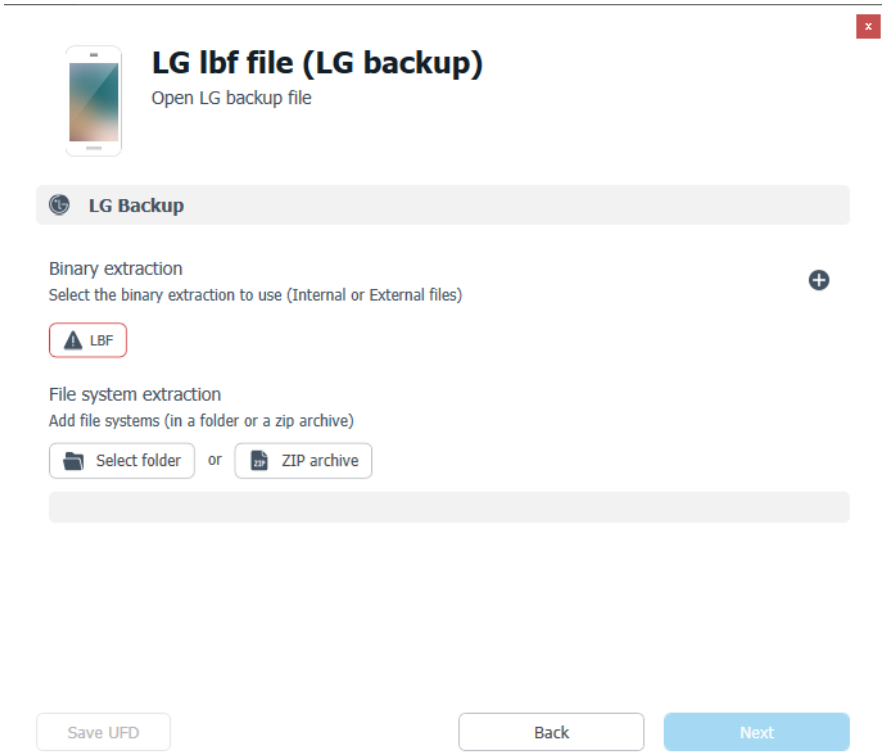
» Select **Common source > Backup > Huawei - Huawei backup.**

Opens Huawei backup data.


Huawei HiSuite or External memory backup
Opens Huawei backup data
Huawei Backup
File system extraction
Add file systems (in a folder or a zip archive)
Select folder
or
ZIP archive
Save UFD
Back
Next

» Select **Common source** > **Backup** > **LG - LG backup (lbf)**

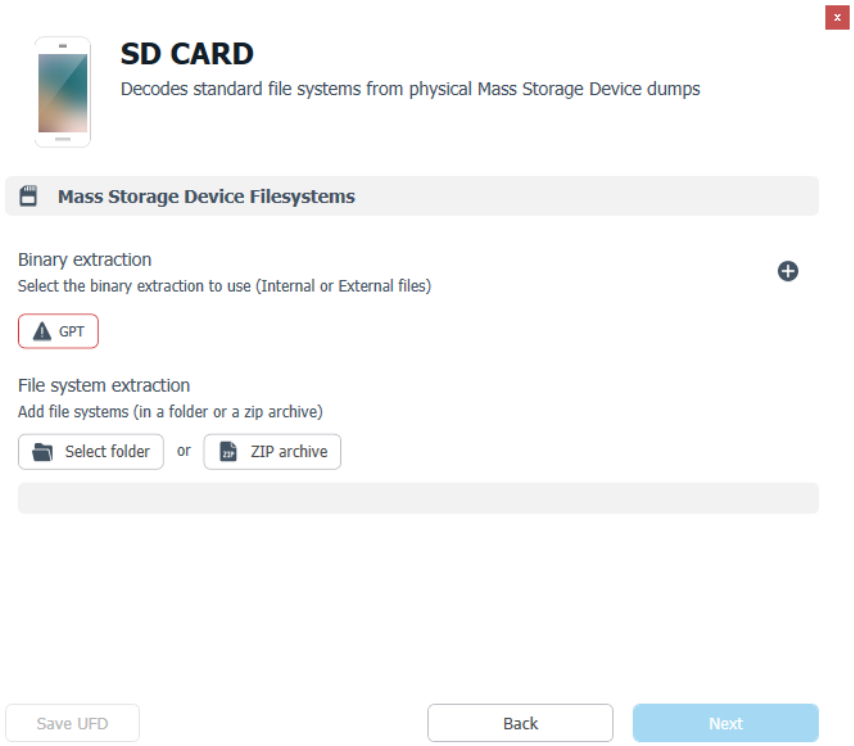
Decodes data from LG Backup files.



4.3.2.4.2. Storage device

» Select **Common source** > **Storage device** > **SD card**

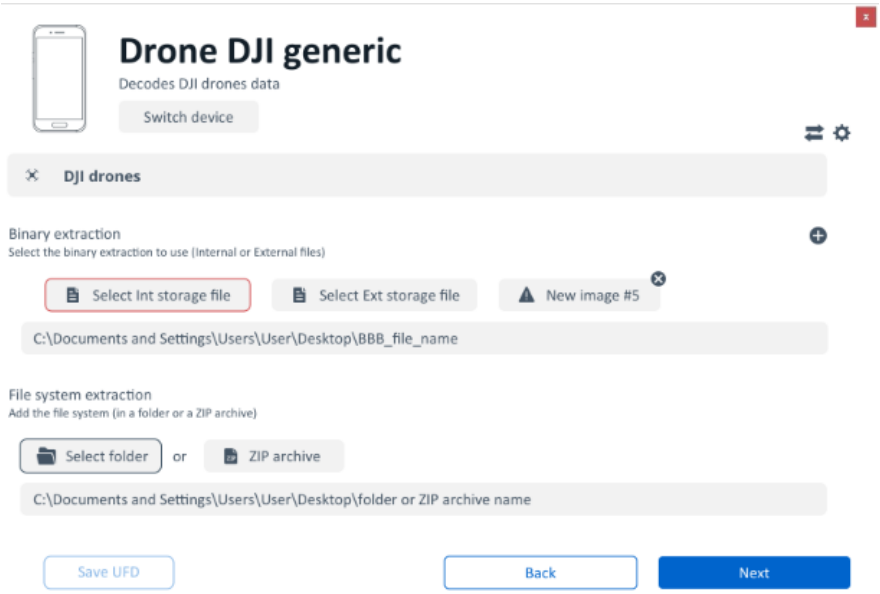
Decodes standard file systems from physical mass storage device extractions.



4.3.2.4.3. Drones

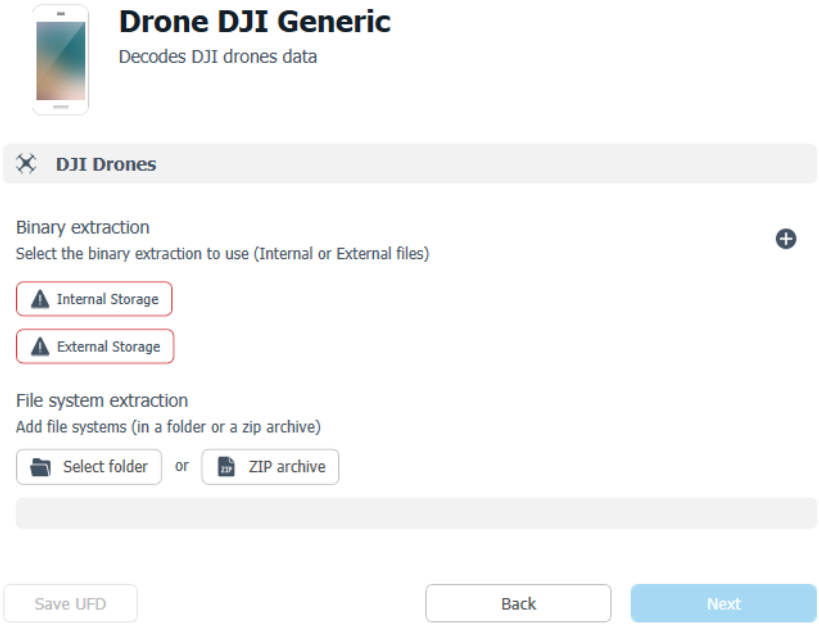
» Select **Common source** > **Drones** > **DJI - DAT files**

Decodes DAT log files from DJI drones including internal and external SD cards.



» Select **Common source** > **Drones** > **DJI Physical extraction**

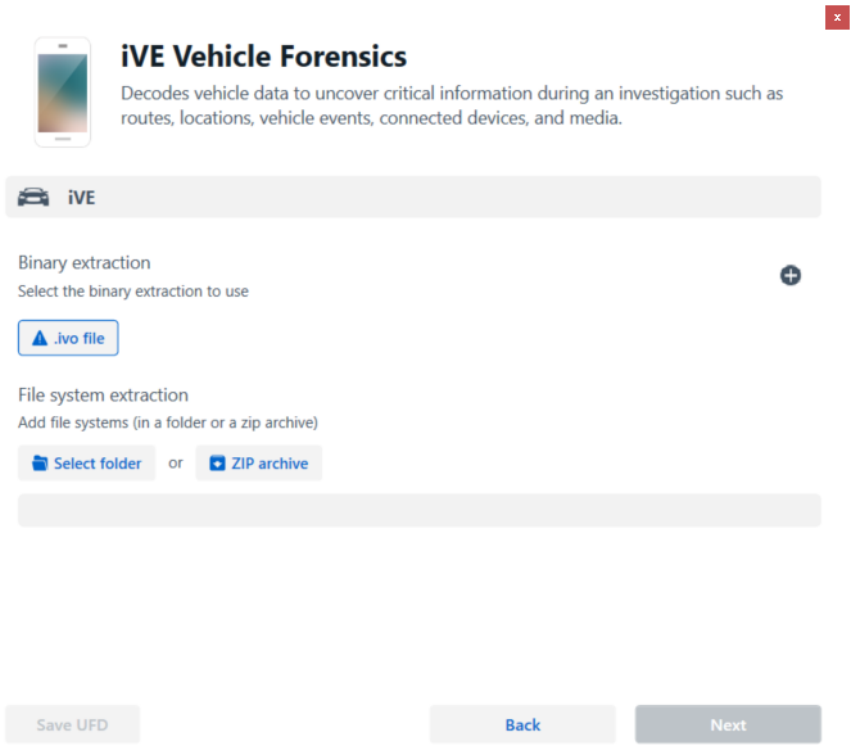
Decodes data from DJI drones including internal and external SD cards.



4.3.2.4.4. Vehicle forensics

» Select **Common source > Vehicle forensics > iVE (.ivo file)**

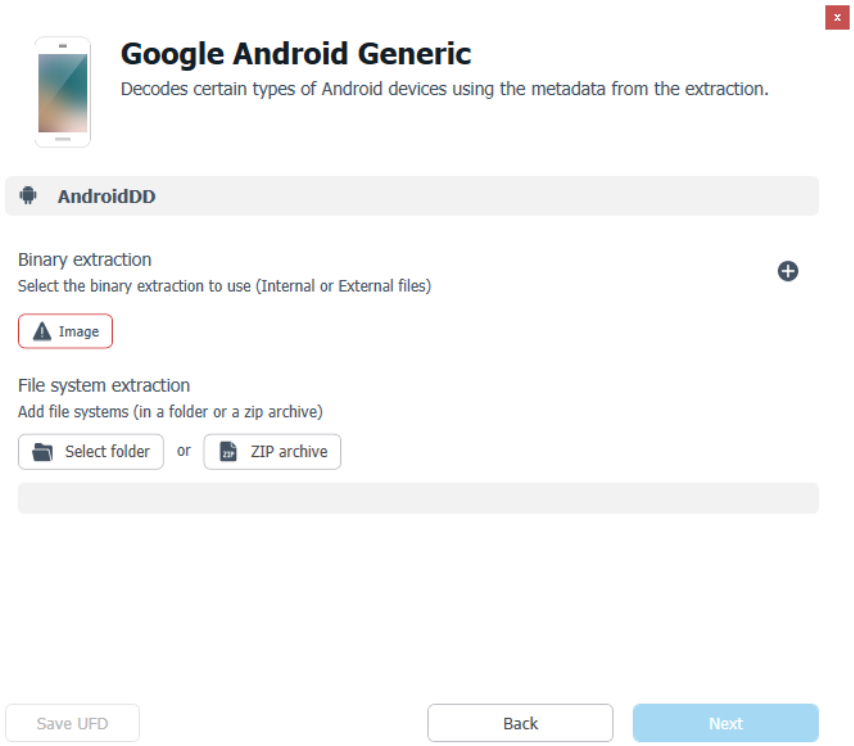
Decodes vehicle data to uncover critical information during an investigation. See Vehicle forensics (on page 66).



4.3.2.4.5. Android emulator

» Select **Common source** > **Android emulator** > **Android .vmdk**

Decodes Android Emulator VMDK files.



4.3.2.5. Vehicle forensics

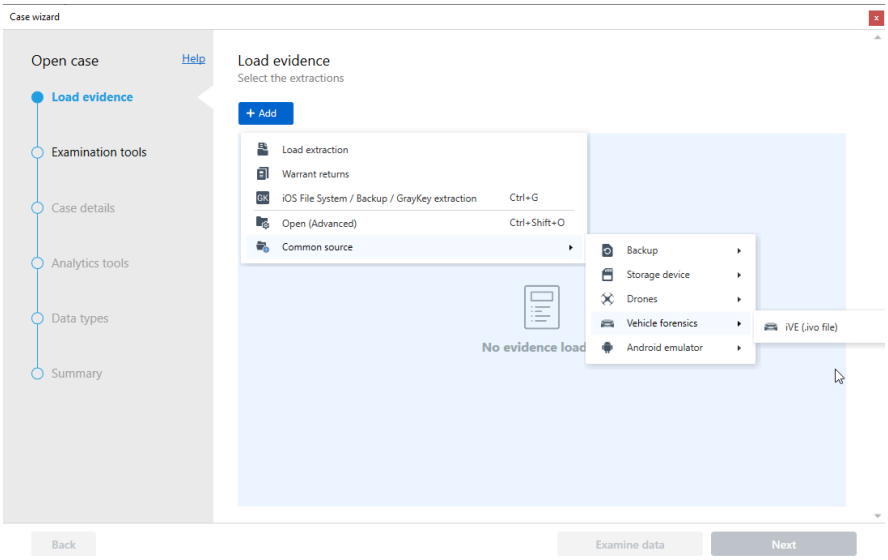
Physical Analyzer can ingest and decode vehicle forensic files (.ivo) to uncover critical information during an investigation.

Ingested data types for vehicle forensics files include:

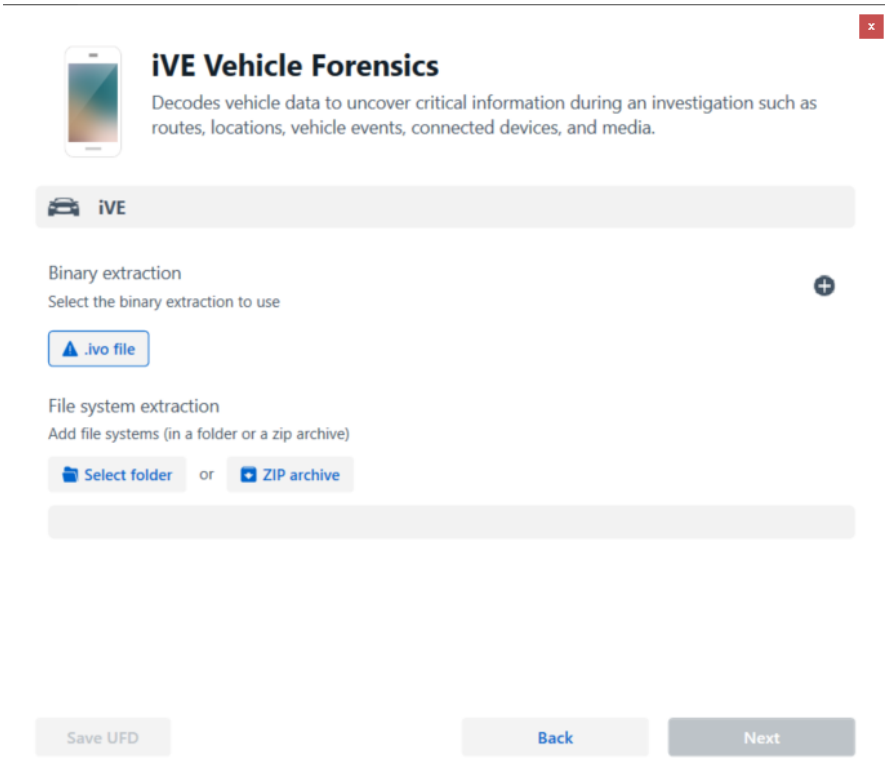
- Call logs
- Contacts
- Databases
- Device info
- Devices
- Journeys
- Locations
- Searched items
- Timeline

To ingest and decode vehicle forensics files

1. Go to **File > Open case.**
2. Click Add.
3. Select Common source > Vehicle forensics > iVE (.ivo file).



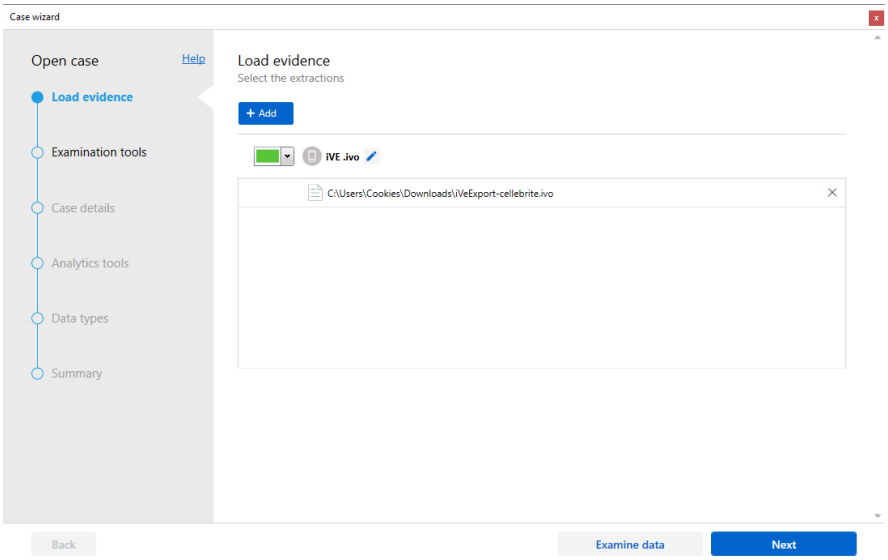
4. In the iVE Vehicle Forensics window, click **.ivo file**.



5. Select file and click Open.
6. Click **Next**.

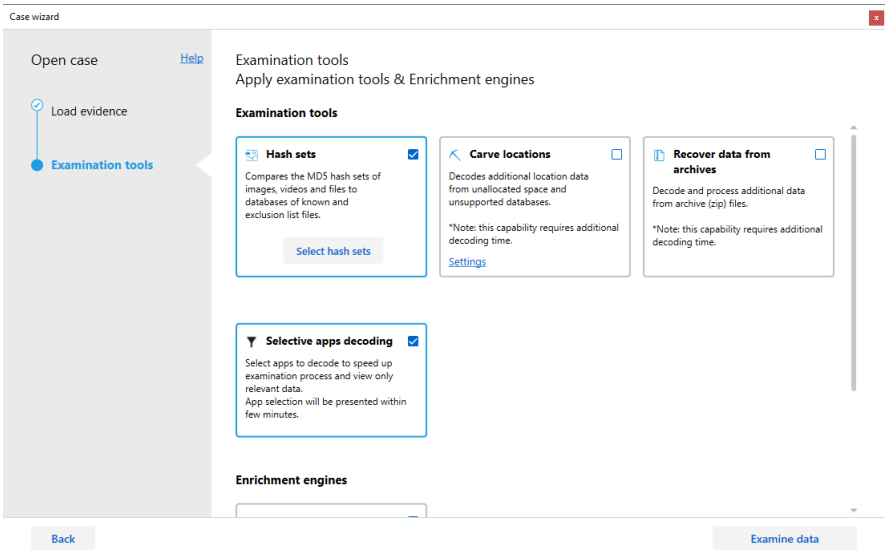
> For File system extractions, click **Select folder** or **ZIP archive**.

7. In the Load evidence screen, click **Next**.



> Click Examine data to skip the next step and begin ingestion.

8. In Examination tools screen, select the tools to run on the device.
9. Click **Examine data**. The decoding begins.



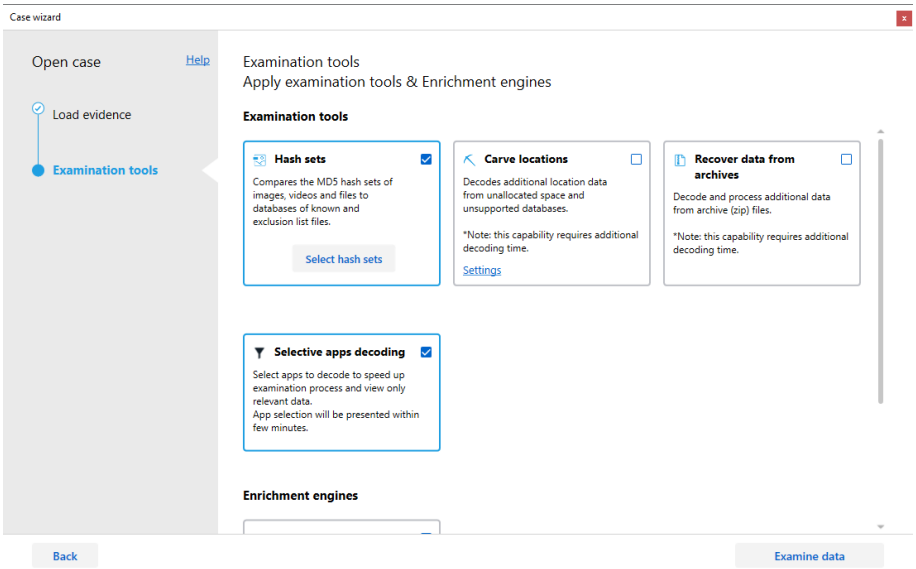
4.3.3. Examination tools

In this step, you select the examination tools before decoding starts to prepare the evidence for the case.

Select from the following examination tools:

- **Hash sets:** Compares the MD5 hash sets of images, videos and files to databases of known and blacklisted files. For more information, see Importing and categorizing hash sets (on page 152).
- **Carve locations:** Decodes additional location data from unallocated space and unsupported databases. For more information, see Carving locations (on page 361).
- **Recover data from archives:** Decode and process additional data from archive (zip) files. This tool requires additional decoding time.
- **Selective apps decoding**: Select apps to decode and review from the apps installed on the examined device. For more information see Selective apps decoding (on page 353).
- **Enrichment engines:** Classify images and videos based on categories relevant to the case. Clicking **Select categories** allows you to select the categories to be included in the classification. For more information, see Media classification (on page 346)

> Running the Suspected CSA category may increase process time and memory consumption. Use a GPU card (NVIDIA® GPU card with CUDA© compute capability 3.5 or higher) to boost the speed of this process.



To select the examination tools to run on the case:

1. Select the required examination tools.
2. Click **Examine data** to start the decoding process.

4.4. Analyzing multiple extractions

The Multiple Extraction feature enables you to merge multiple extractions into a single project providing unified analysis (views and reports). This feature saves time and reduces the effort required to review different types of extractions with the same data.

You can open UFDX files separately, with extractions in different projects, or you can open a single project with all extractions presented under one unified project. You can merge any of the following extractions: logical, file system, physical, SIM, JTAG, memory card, camera, and open advanced.

This feature decodes and analyzes a single unified project, and can remove deduplications (duplicate or redundant information). The extracted data is presented under one project tree providing the following:

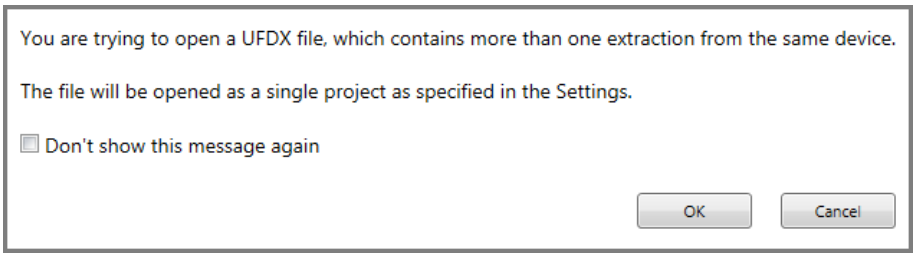
- A unified Extraction Summary and Device Info, with the ability to drill-down to each extraction.
- A source extraction per any record.
- Deduplications are grouped together to enable quick and efficient analysis.
- Filtering capabilities. See Using the quick filter (on page 135).
- A unified report of all merged extractions, with an indication of the original extraction source.

4.4.1. Opening and merging projects

You can add any type of extraction to an existing project. You can open a UFDX file that contains a number of extractions, or you can add extractions to an existing project.

Open a UFDX file as a multiple extraction project:

1. Select **File** > **Open** or click the Open button ( ) and select the EvidenceCollection.ufdx file. (This file is created when you have multiple extractions for a single device.) The following window appears.



2. Select the **Don't show this message again** check box if you do not want this message to be displayed each time you open a UFDX file with multiple extractions.
3. Click OK.

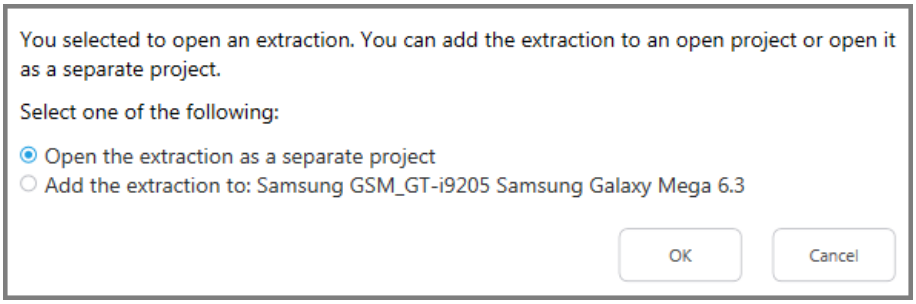
To add an extraction to an open project:

1. Click the **Add extraction** button

or right-click the project and select **Add Extraction**.
2. Select the required extraction.
3. Click OK.

To open an extraction:

1. Select **File** > **Open** or click the Open button ( ) and select the file to open. The following window appears.



2. Select to open the extraction as a separate project, or select to add the extraction to an open project.
3. Click OK.

To save the multiple extraction project:

» Select **File** > **Save as UFDX**.

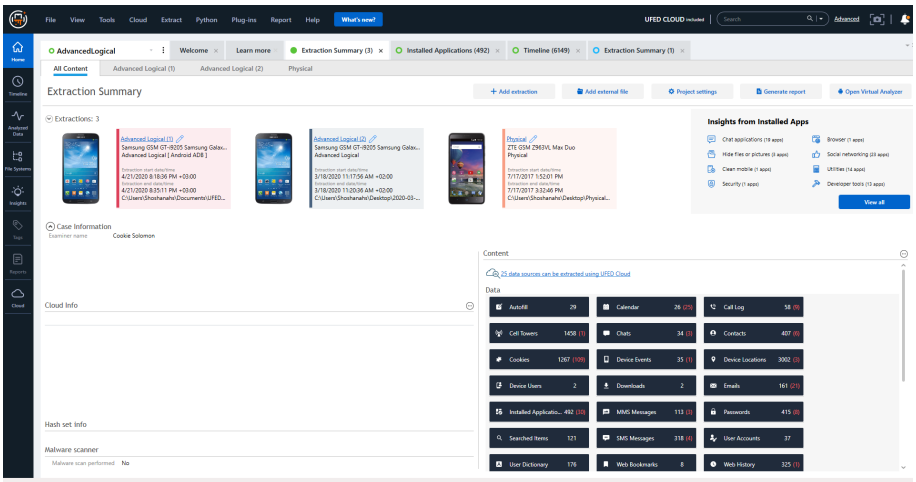
To close all the tabs of a multiple extraction project:

» Select **File** > **Close tabs** and select the project.

4.4.2. Extraction Summary

The Extraction Summary area in the project tree includes all extractions included in the multiple extraction project. Each extraction appears in a different color, which helps you identify the origin of the data in the various Analyzed data tabs.

The Extraction Summary tab includes a summary of all the extractions in the All Content tab and there is a separate tab for each extraction. An example of a multiple extraction project is displayed next.



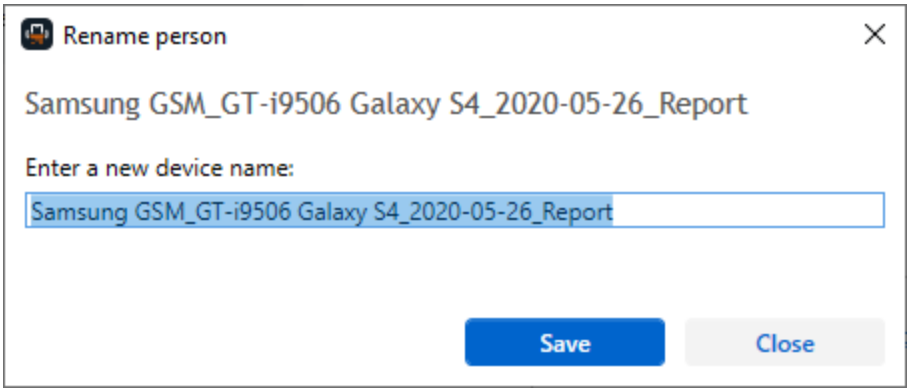
For more information regarding the data presented in the Extraction Summary tab, see Extraction summary tab (on page 98).

4.4.3. Renaming projects and extractions

When a project with multiple extractions opens the project is called Multi-project. You can rename this project. You can also rename the default names of the extractions in the project. For more information on renaming extractions, see All Content tab (on page 98).

To rename a project:

1. Click ⋮ next to the project name.
2. Select **Rename**. The following window appears.



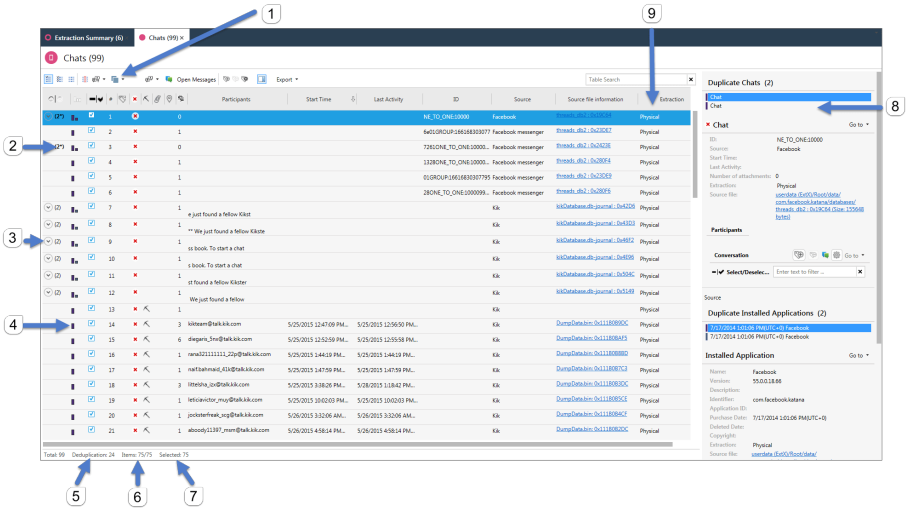
3. Enter the required name for the device.
4. Click **Save**.

4.4.4. Decoding and analysis

Decoding is initiated on the multiple extraction project, allowing deduplications to be displayed or filtered out. All extracted data is presented under one project tree.

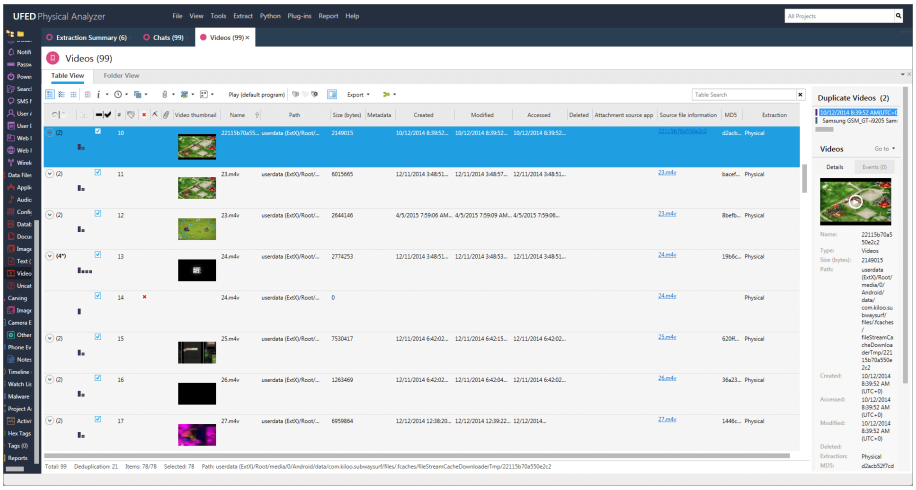
In the Analyzed data area, you can see deduplications and the bar graph indicates the source extraction for the data. The colors of the bars match the colors of the extractions in the Extraction summary tree area. If required, you can change the settings to remove deduplications. For more information, see General settings (on page 421).

The following example from the Analyzed Data area shows information that is relevant to a multiple extraction project.



1. Related items filter.
2. The * indicates that additional information is available within one of the merged items.
3. Item with deduplications.
4. Source extraction icons.
5. 24 items include deduplications.
6. View shows 75 of 75 selected items.
7. 75 items selected.
8. Additional information can be viewed here.
9. The extraction from which the data was derived.

The following example from the Data Files area shows information that is relevant to a multiple extraction project.



4.4.5. Multiple extraction settings

When using a multiple extraction project, the following settings in the General Settings area can be used:

- Automatically adjust timestamps to UTC+0
- Automatically adjust timestamps according to the device's time zone
- Open a UFDX file as a multi project
- Remove duplicates

For more information on these settings, see General settings (on page 421).

4.4.6. Reporting

You can generate a unified report for a multiple extraction project, with an indication of the original extraction source. For more information on the reporting settings that are applicable to multiple extractions, see "Include merged items (analyzed data)", "Include merged items (data files)" and "Include source info" in Generating a report (on page 257).

4.5. Saving a project session

Save the project session to save your work on the project, enabling you to close Physical Analyzer and restart your session at a later time.

The saved session file (.pas) includes:

- User selection in the **Analyzed Data** and **Data Files** tables
- Case Information settings
- Generated reports
- Hex tags
- Location address
- Opened tabs
- Project name
- Project settings
- Report selection
- Searches
- Tags
- Translations
- Unified time zone settings
- User sorting in data tables
- Verifying hash values
- Watch list results

A project session can also be created for extractions performed by third party tools.

Saved project sessions do not contain defined settings. For more information on how to save your settings, see Saving settings (on page 445).

To save a project session:

1. In the **File** menu, select **Save project session**. The Save As dialog box appears.
2. Browse to the location where you want to save the project session file.
3. To change the file name, edit the automatically assigned name in the **File name** box.

> To overwrite an earlier session, choose the same file name.

4. Click **Save**.

4.6. Adding external files

If required, you can include related artifacts in your case. These are external files such as search warrants, additional images and relevant documents. These files will be added to the project tree, under Additional files and can be included in reports.

To add external files to the report:

1. Click **Add external files** in the Extraction Summary.

   or

   Click ⋮ next to the project and select **Add external file**.

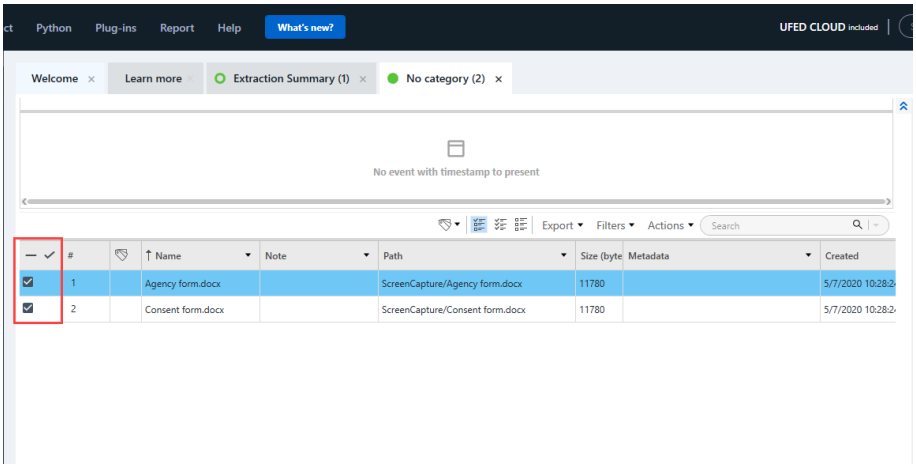
2. Select the file. The following window appears.

3. Enter a name for the file.
4. Enter or select a category.
5. If required enter any notes.

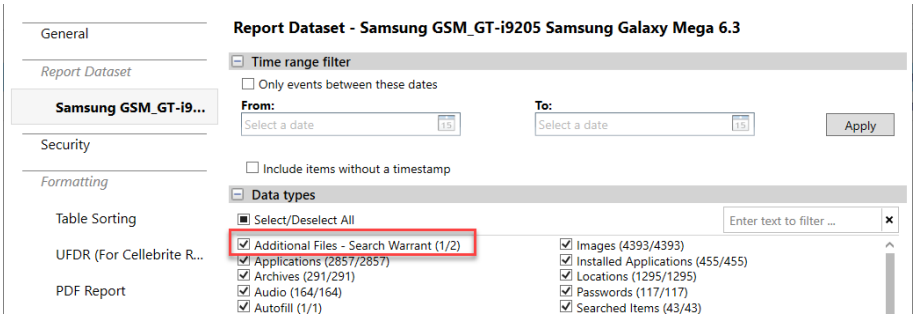
> For images, you can use the drawing tool on the left to draw text, add shapes, crop, resize, rotate, and flip the image. You can also copy the image to the Clipboard.

6. Click **Add to project** and select the project. The file is located in **Reports > Additional files > External files**.

7. Open the files from here and select or clear the check box to include or exclude files from the report.



8. When generating a report select the **Additional Files** check box.



4.7. Loading a project session

1. From the **Welcome** tab, open the project that you want to work in.
2. In the **File** menu, select **Load project session**.
3. In the Open dialog box, browse to and select the project session file that you want to open.
4. Click **Open**. The session opens.

4.8. Closing a project

- Do one of the following:
  - In the **File** menu, select **Close**.
  - Right-click the project name in the **Project tree** and select **Close**.

4.9. Closing Physical Analyzer

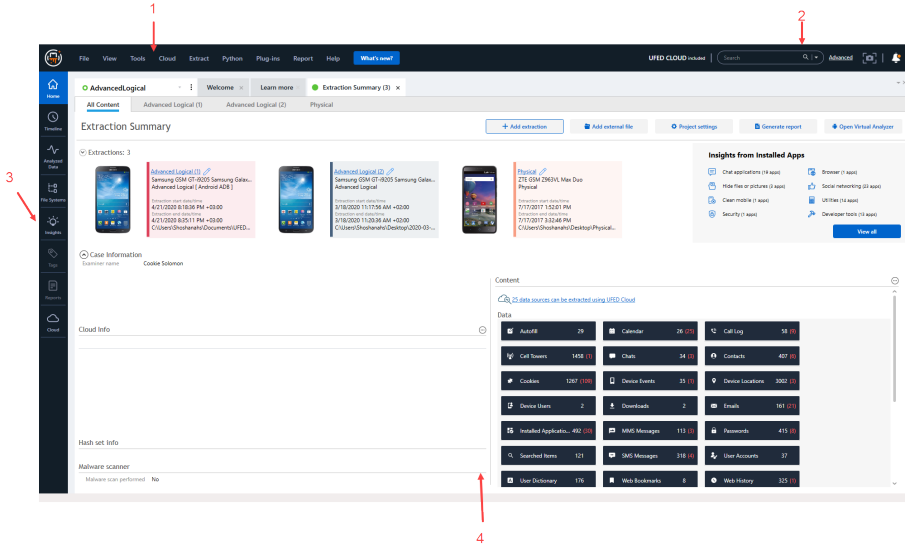
- In the **File** menu, select **Exit**.

4.10. Keyboard shortcuts

Ctrl+B	Add an entity bookmark
Ctrl+D	Select a folder for the dump file system
Ctrl+E	Export an account package
Ctrl+End	Move the cursor to the end of a table
Ctrl+H	Open the hash set manager
Ctrl+K	Open the Watch list editor
Ctrl+H	Run the Watch list
Ctrl+H	Open the hash set manager
Ctrl+M	Export the hash database
Ctrl+Home	Move the cursor to the beginning of a table
Ctrl+I	Open iOS device extraction wizard
Ctrl+J	Extract GPS or mass storage device
Ctrl+O	Open a file
Ctrl+P	Open project settings
Ctrl+Q	Open the SQLite query manager
Ctrl+R	Open the report wizard
Ctrl+V	Load the Android Emulator
Ctrl+Shift+O	Open advanced
Ctrl+T	Open settings
Ctrl+Tab	Switch between open tabs
Ctrl+U	Open the UFED Downloader to connect to UFED
Ctrl+W	Close a project
F1	Open the product documentation
Space	Select or clear check boxes
Ctrl+F6	Redact images or videos

5. Orientation to the workspace

The workspace contains two main areas; the project tree and the data display area to streamline your workflow.



The workspace contains the following components:

1. Application menu bar
2. All projects search
3. Navigation Menu
4. Data display area

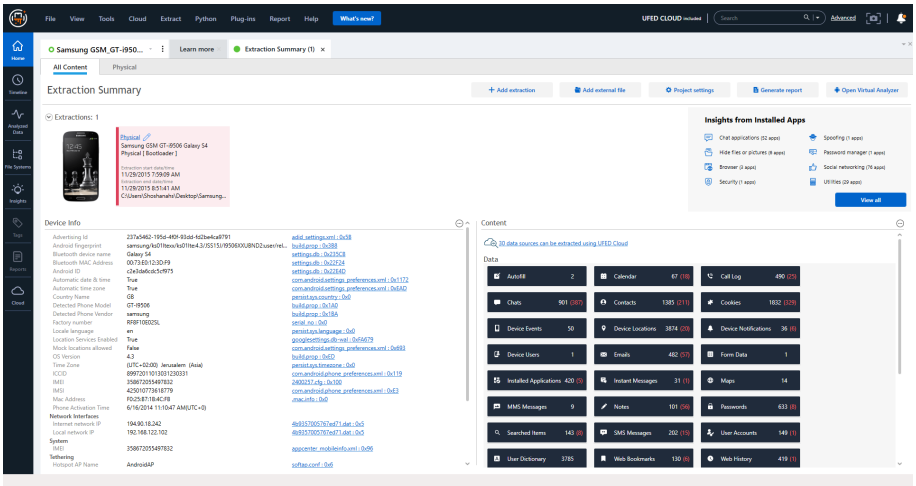
5.1. Navigation menu

Navigate the Physical Analyzer application views from the following navigation menu items:

- Home
- Timeline
- Analyzed data
- File Systems
- Insights
- Tags
- Reports
- Cloud

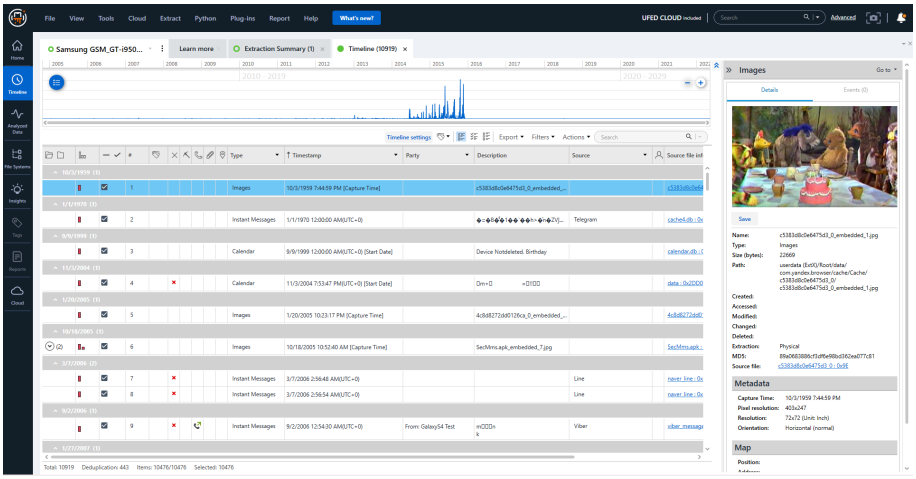
5.1.1. Home

The Home view displays the Extraction summary. See Extraction summary tab (on page 98).



5.1.2. Timeline

Timeline view is a powerful tool that enables you to analyze data in chronological order, to identify the order of events and make connections between them.



Filtering and sorting the timeline table

The timeline has many advanced filtering and sorting options to drill down to specific data and display them according to the users needs.

Filter by Type, Timestamp, Party, Description, Source, Source file information, and Extraction.

To filter the timeline:

1. Click the dropdown icon in a column heading.
2. Select the filter options
3. Click **Ok**.

To clear applied filters, click **Clear filters**.

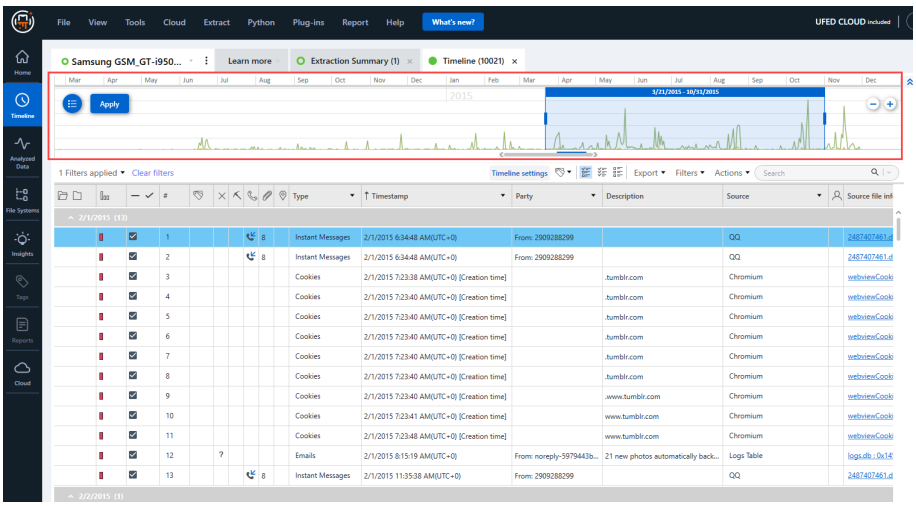
Sorting the timeline table

Sort the timeline table by Type, Timestamp, or Extraction.

1. Click the dropdown icon in a column heading.
2. Select either:
   - Sort ascending
   - Sort descending

The graphical timebar

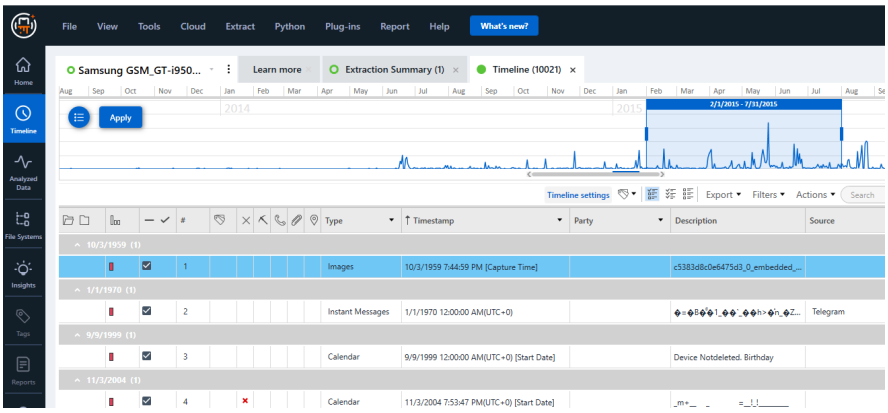
The graphical timebar allows you to zoom-in to the timeframe in question as well as analyze multiple timestamps of events.



To select a specific timeframe in the graphical timebar:

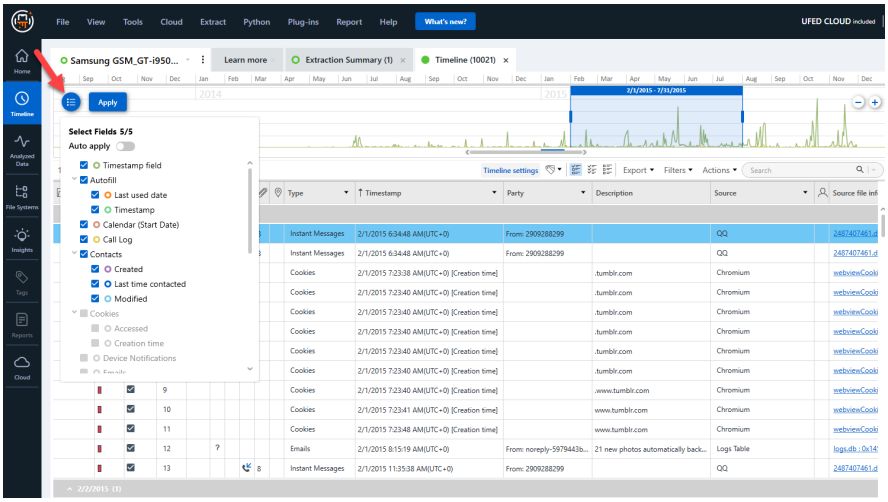
1. Click and drag on the time bar to select a timeframe.
2. Click **Apply**.

   The table is updated to reflect the selected timeframe.



To apply fields to the graphical timebar:

1. Click to open the fields selection window.
2. Select the required fields.
3. Click **Apply**.

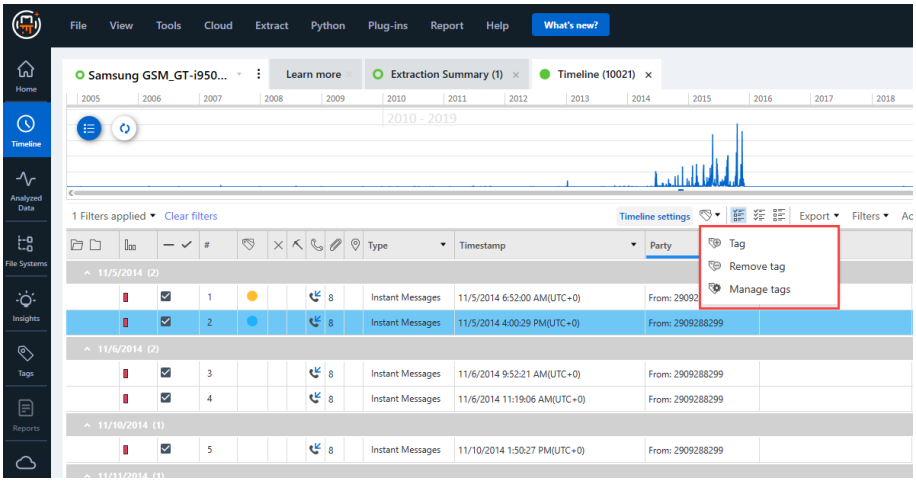


To zoom in the graphical timebar click . To zoom out, click .

To clear timebar settings, click **Clear**.

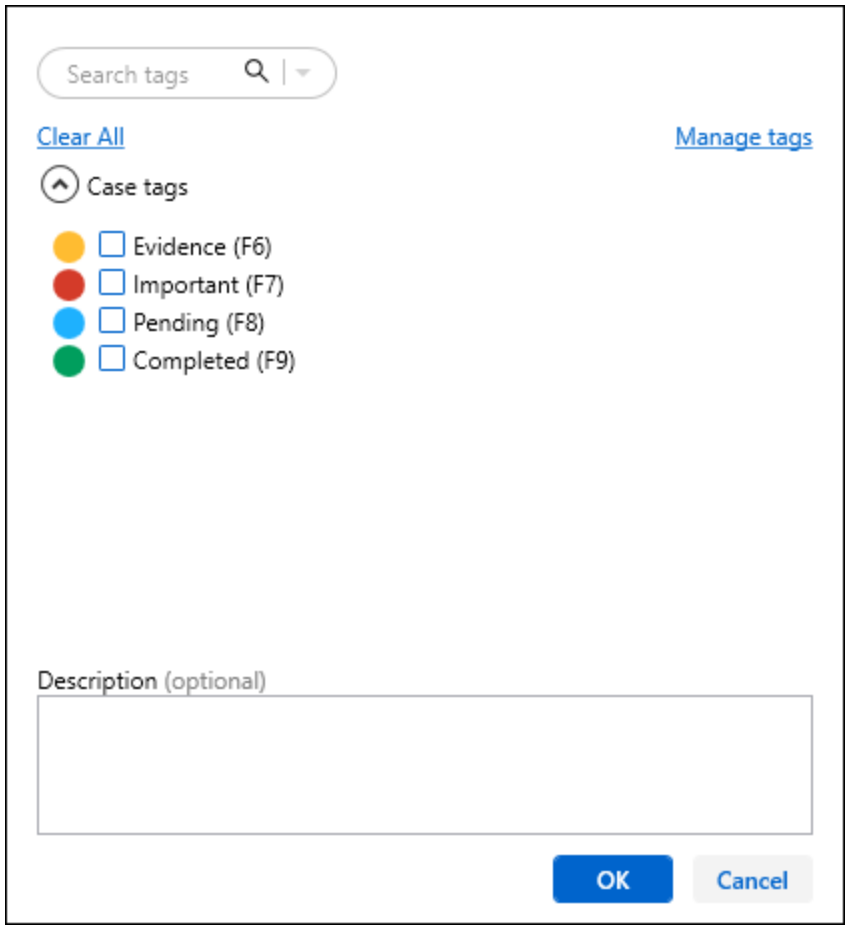
Tagging items on the timeline

Tag timeline items for easier data management.



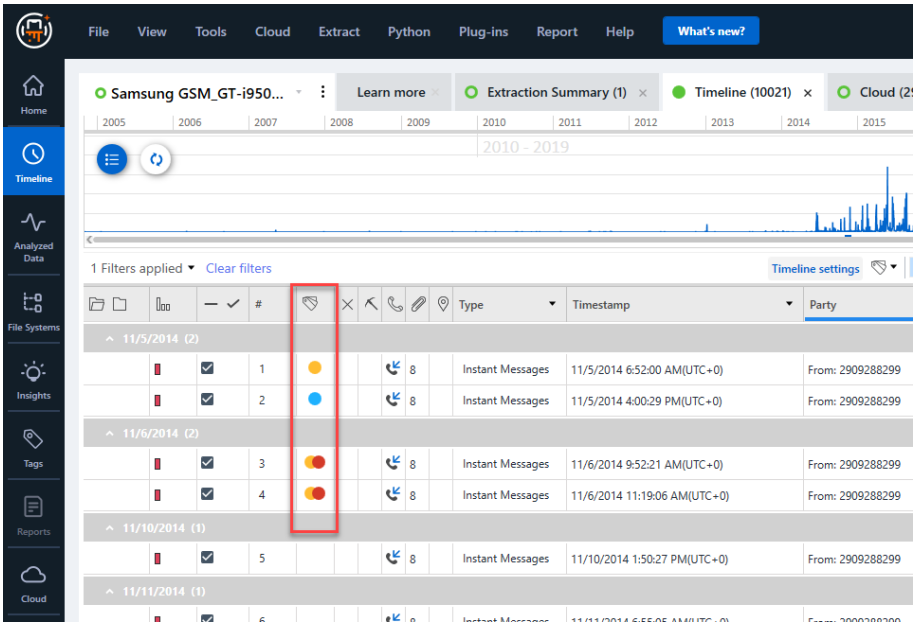
To add a tag to timeline items:

1. Select one or more row in the timeline table.
2. Click .
3. Select **Tag**.
4. Select the required tags.



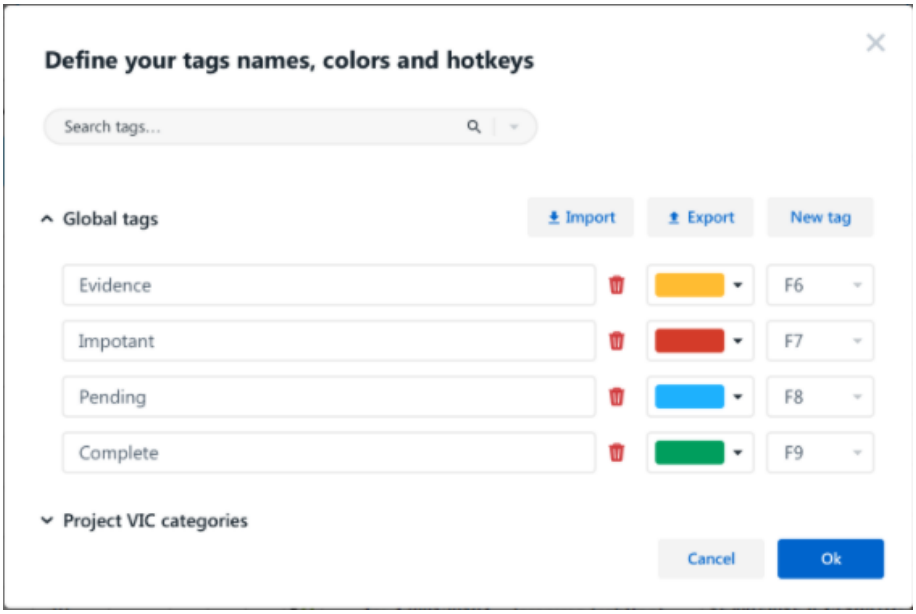
5. Click **OK**.

The Tags column is updated with the selected tabs.



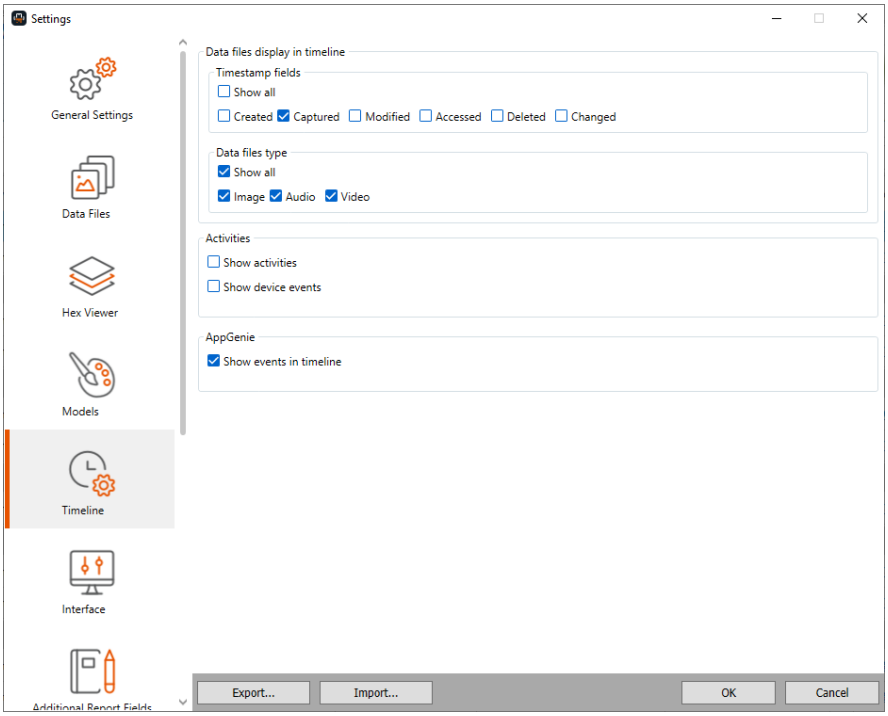
To manage tags:

1. Click .
2. Select **Manage tags** .
3. In the Manage tags window you can:
   - Search tags.
   - Rename existing tags.
   - Delete tags.
   - Define tag color.
   - Define tag hotkey.
   - Create a new tag by clicking **New tag**.
   - Export and import list if tag labels.
4. Click Ok.



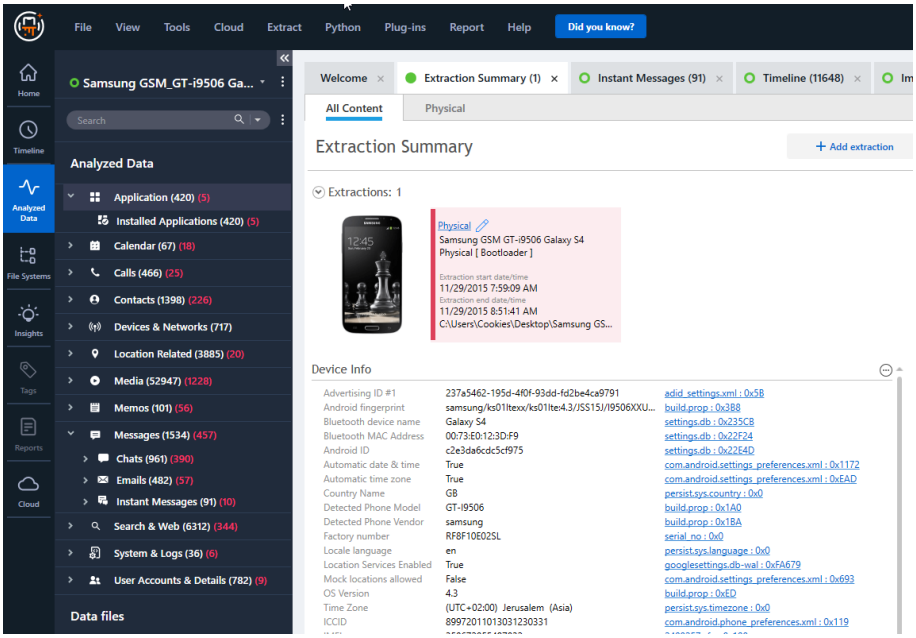
Managing timeline settings

1. Click **Timeline settings**.
2. Select required settings.
3. Click **Ok**.



5.1.3. Analyzed data

The **Analyzed Data** view displays a tree with groups of analyzed data that are related to device-specific features such as contacts, Instant messages, call logs, and so on.



The available information and what is displayed depends on the device features and application version. For example mail messages are sorted according to the account through which they were sent or received. An uncategorized account or messages folder lists the folders or messages that cannot be categorized in any of the found accounts or account folders (Inbox, Outbox, Drafts, and so on).

The following information types are displayed in the Analyzed data tree:

Analyzed Data

- **Personal information** - Calendar, contacts, notes, call log, user dictionaries, user accounts.
- **Messaging items** - Email, instant messages, chat[1].
- **Web browser items** - Bookmarks, history, cookies.
- **Media items** - Audio, images, and videos.
- **GPS information** - Locations (including from video files, metadata, and SQLite databases), journeys, fixes. For more information on geolocations, see Device locations (on page 170).
- **Public transit ticket** - Public transportation ticket information discovered in the extraction.

---

[1]In some cases, mainly when messages have been deleted, they cannot be forensically placed in a Chat. To maintain forensic accuracy of the messages, they will be placed in Instant messages and available for review under **Analyzed data > Instant messages**.

- **Physical activities** - Physical activities performed by the owner as well as health related measurements including heart rate, blood pressure, etc.
- **Device information** - Bluetooth pairings, wireless networks, SIM data, application usage, Wi-Fi, cellular locations.

The number in parenthesis designates the number of items each category contains.

Selecting any analyzed data category automatically adds it to the highlights list of the displayed binary image and/or memory range it belongs to (located at the bottom of the Hex view tab), and highlights its data range portions in the displayed data.

Data files

The Data Files tree item sorts the extracted data into common formats, used by devices and computers, such as text or document files.

In the project tree, the information is displayed in the following categories:

- **Applications** - Files that were recognized as application files (such as .apk, .jar, .dex, .so, .exe)
- **Archives** - Files that were recognized as archive or compressed files (such as .zip, .zipx, .rar, .tar, .gzip, .7zip, .7z, .dar, .gz, .arj)
- **Configurations** - Device configuration files (such as iOS plist files)
- **Databases** - Data structures that were recognized as databases
- **Documents** - Files that were recognized as document file formats (such as .doc, .docx, pdf; xlsx, ppt).
- **Shortcuts** -
- **Text** - Files that were recognized as text file formats
- **Uncategorized** - All unknown file formats or undefined file extensions.

Deleted items are indicated in red.

You can create additional data file groups. For more information, see Managing data files settings (on page 430) .

Double clicking on a tree item opens a tab in the data display area.

Expand or collapse tree items by clicking ⋮ and selecting **Expand all** or **Collapse all**.

5.1.4. File systems

The File systems view displays a tree with the following data:

- **Memory images** - Double-click an image item to display it in a Hex View tab in the data display area.

  The **Memory Images** - tree item lists all the extraction files generated from the memory modules of the device.

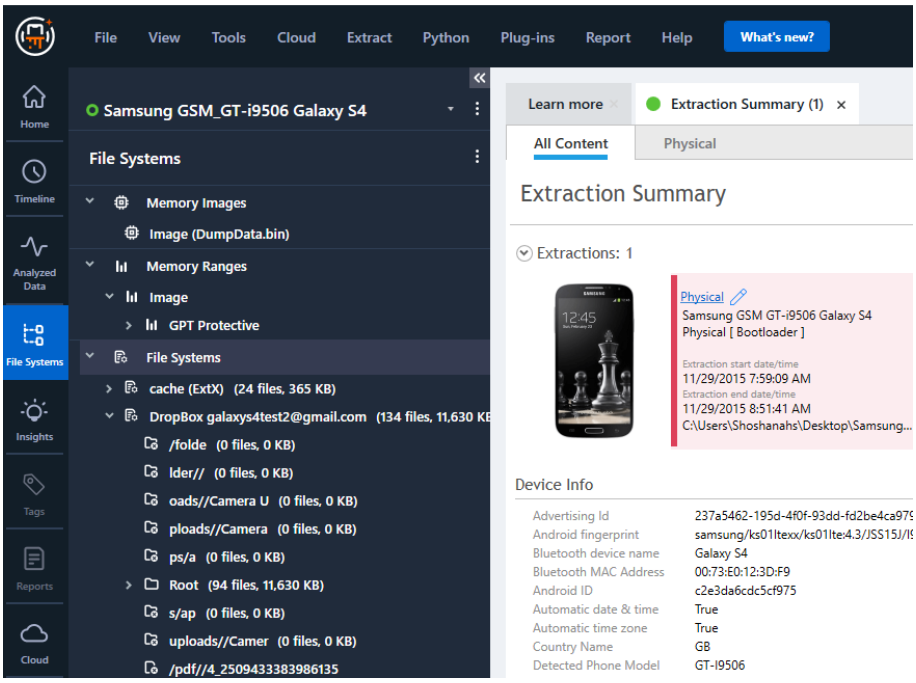
- **Memory Ranges** - lists the analyzed memory ranges for each of the extracted memory modules of the device (listed under **Images**).

  Select a memory range to:

  - Highlight the memory range portion in the displayed data
  - Add it to the highlights list of the displayed binary image it belongs to (located at the bottom of the Hex view tab).

    Double-click a memory range item to display its content in a new Hex view tab.

- **File systems** - file systems found or reconstructed out of the analyzed binary file.



The **File Systems** tree displays all the file systems found or reconstructed out of the analyzed binary file.

Each file system is marked with (hard drive icon). Deleted files are marked with (red cross icon).

Double-click any file system item to display its content in a new Hex view tab.

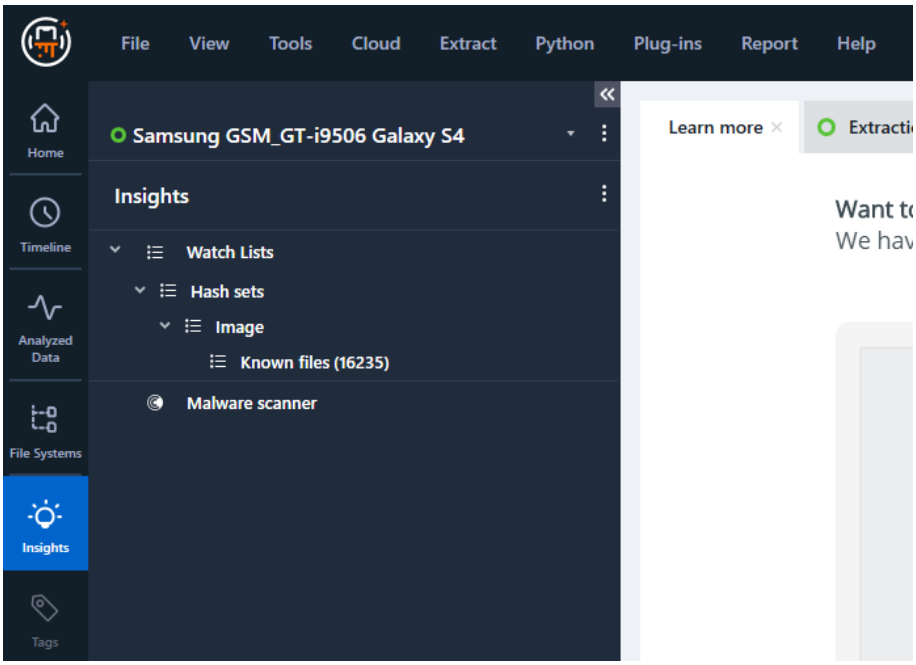
> Double clicking on a tree item opens a tab in the data display area.

Expand or collapse tree items by clicking ⋮ and selecting **Expand all** or **Collapse all**.

5.1.5. Insights

The Insights view displays a tree with the following information:

- Watch lists - Watch lists are lists of keywords that you create and then use to search and identify events and items of interest in the extracted data.
  - Expand **Watch Lists** to view a list of watch lists that have been run in the current session.
  - Double-click on **Watch Lists** to view the highlighted entity based on the watch lists. For more information, see Working with watch lists (on page 145).
- Hash sets
- Malware scanner - Run the malware scanner to identify malware on the device. For more information, see Scanning for malware (on page 29).



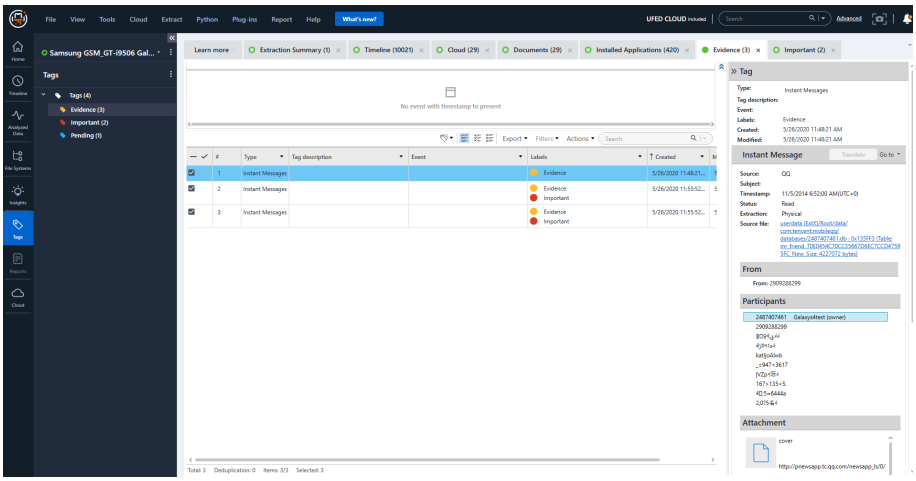
Double clicking on a tree item opens a tab in the data display area.

Expand or collapse tree items by clicking ⋮ and selecting **Expand all** or **Collapse all**.

5.1.6. Tags

The Tags view displays a tree with defined project tags.

Double click on a tag in the tree to open a tab with details in the data display area



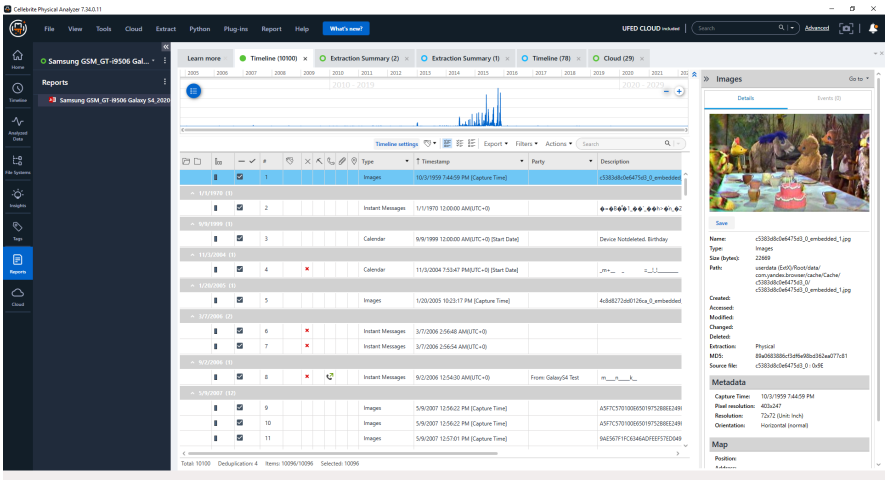
Double clicking on a tree item opens a tab in the data display area.

Expand or collapse tree items by clicking ⋮ and selecting **Expand all** or **Collapse all**.

5.1.7. Reports

The Reports view displays a list of generated reports. See Generating a report (on page 257).

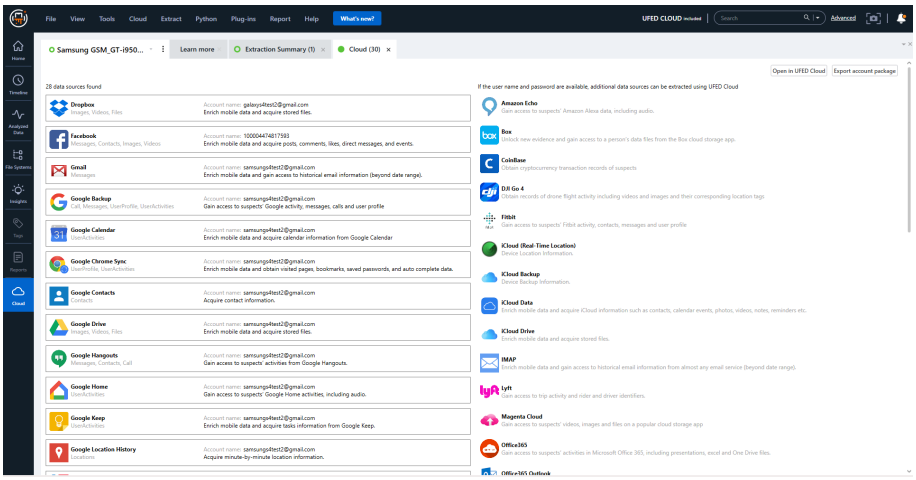
1. Double Click on a report to open. The report opens in the application associated with the report format.



5.1.8. Cloud

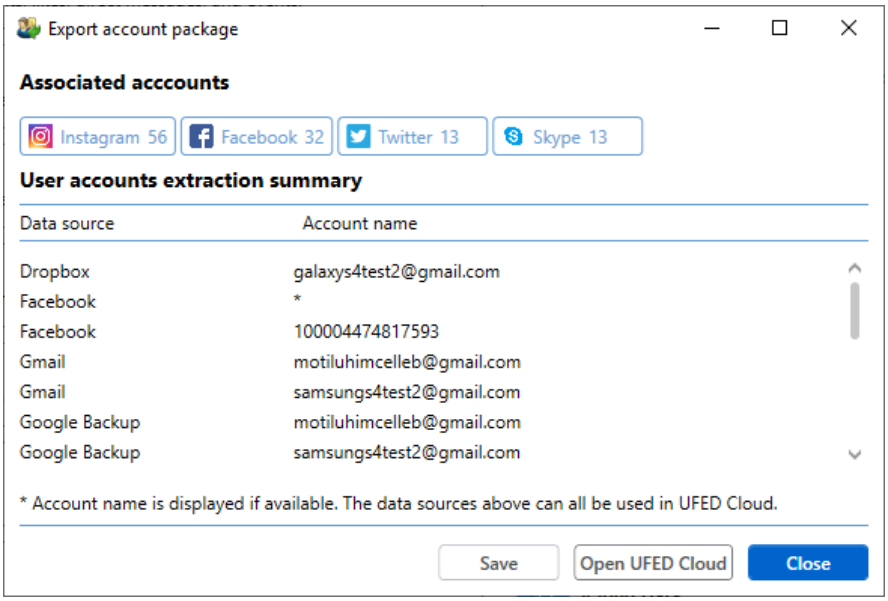
The Cloud view displays all cloud data sources found in the extraction, as well as additional cloud data sources which can be extracted with UFED cloud when username and password are available. See Cloud extractions (on page 208)

It is also possible to export an account package from the Cloud view.



To export an account package

1. Click **Export account package.**
2. Choose the required location to save the file.
3. Click **Save**. The Export account package window appears.



4. Select either:
   - **Save** - to save the account package file
   - **Open UFED Cloud** - to open the account package in UFED Cloud.

     *This option is only available if UFED Cloud is installed on the same machine as Physical Analyzer.

Click **Open in UFED Cloud** to open the UFED Cloud case wizard.

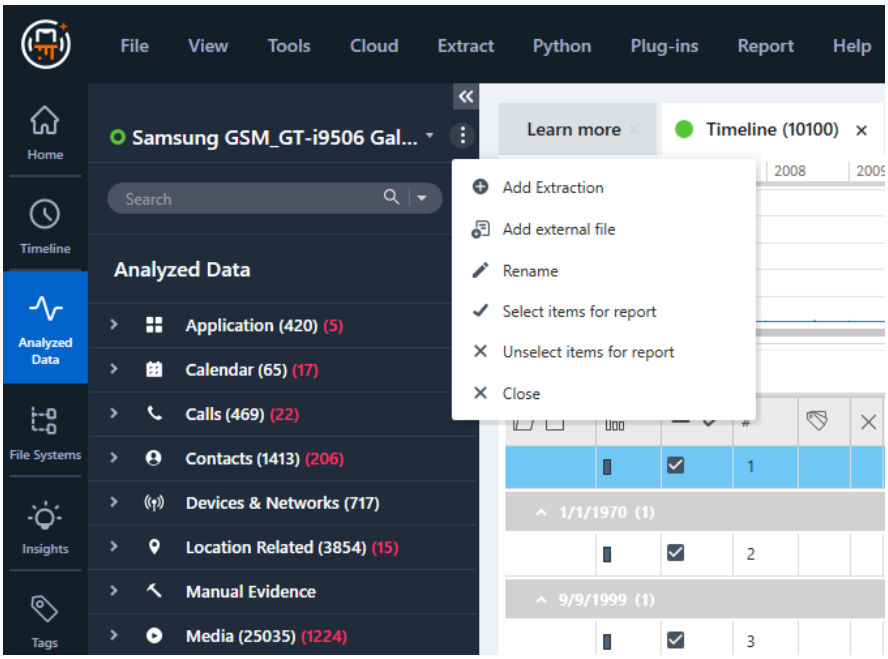
5.1.9. Managing project actions

The project menu allows you to perform the following actions:

- Add extraction
- Add external file
- Rename
- Select items for report
- Unelect items for report
- Close

Procedure:

1. Click the menu icon next to the project name.
2. Select the required menu item.

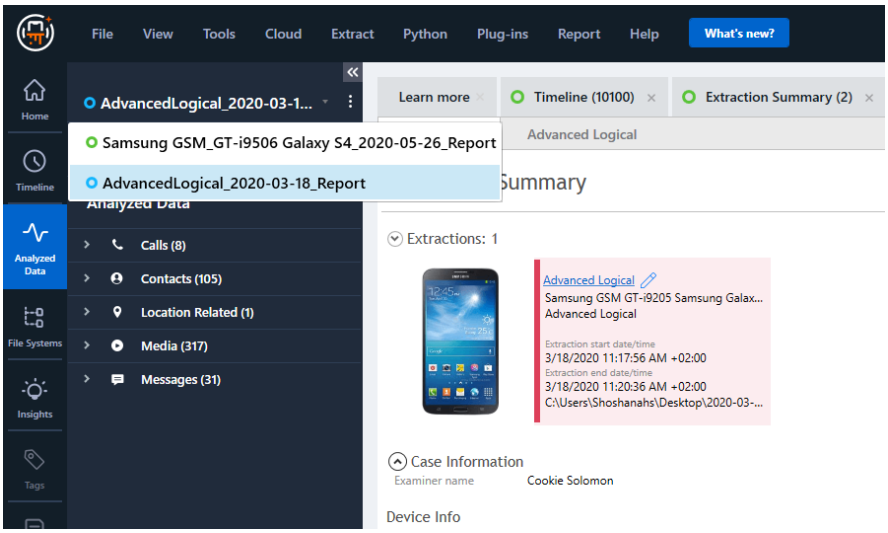


5.1.10. Viewing extraction data from multiple projects

When there are multiple projects open in Physical Analyzer, it is possible to switch between projects to view the data.

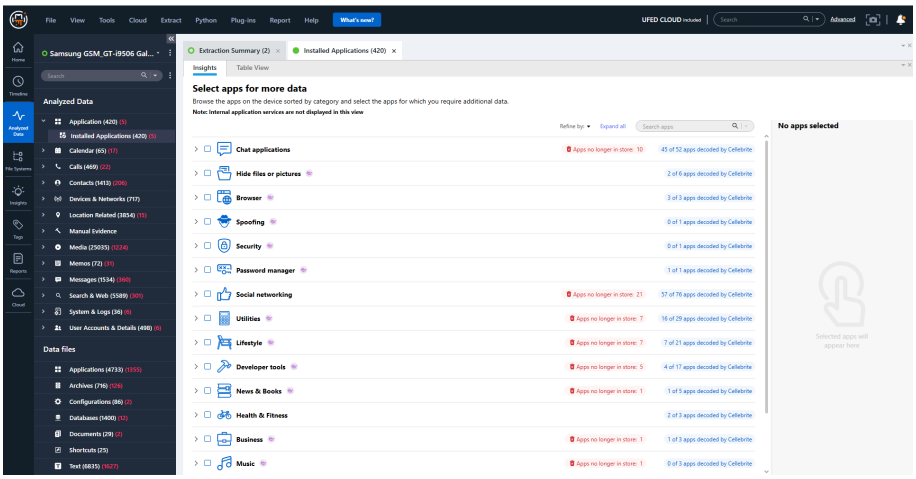
1. Click the dropdown icon next to the project name.
2. Select a project.

   The view displays the extraction data for the selected project.



5.2. Data display area

Double-click an item to display it in a tab. A new tab is opened for each item.



The data display area also displays additional windows such as the Trace window, and Watch list results.

To close a tab, do one of the following:

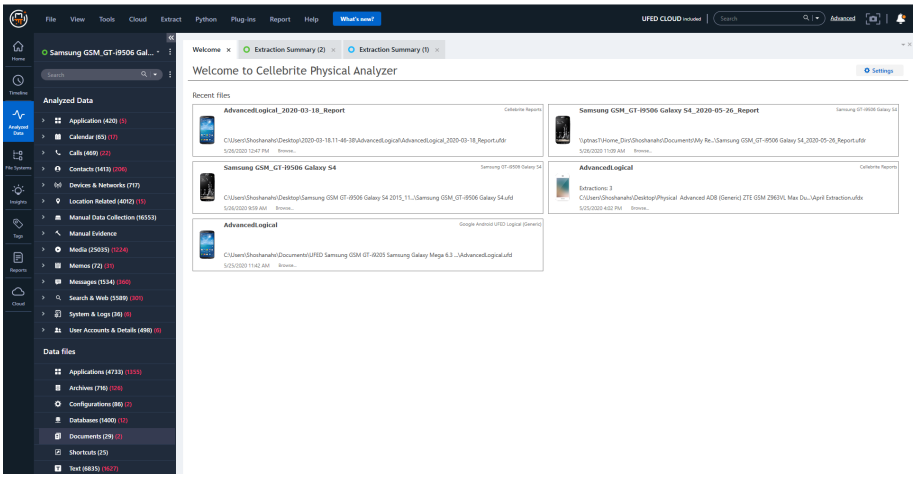
- Click ✕ on the tab header.
- Click ✕ at the top right of the data display area.

To jump to a specific tab either:

- Click on the tab header.
- At the top right of the data display area, click ▾, and select the desired tab from the open tabs list.

5.2.1. Welcome tab

The **Welcome** tab is automatically displayed in the data display area when the application starts and displays a list of recently opened files.



Each file in the list is displayed as a framed information group that contains the following items:

- **Device picture** - A thumbnail image of the device from the application resources, if available. When unavailable, a general placeholder image is used.
- **File name** - The name of the opened file, without the file extension.
- **File path** - The file system path to the file location.
- **Device model** - The identified device manufacturer and model, or BINARY if the opened file was a binary extraction.
- **Date and time** - The date and time stamp in which the file was last opened.
- **Browse link** - A direct link to the file in the system.

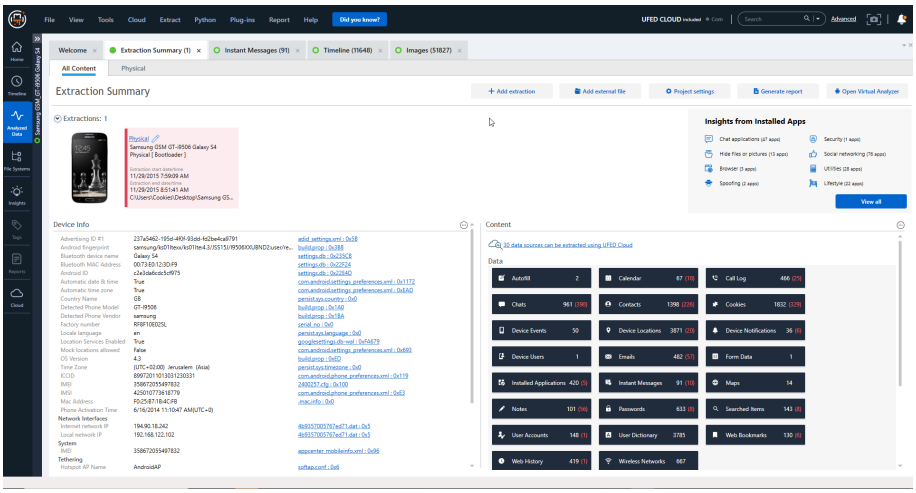
> To remove a recent item from the Welcome tab, click ✕.

You can do the following:

- Click on a framed item to open the files for decoding.
- Click **Browse** to go directly to the file associated with it in the file system.
- Close the **Welcome** tab. To reopen it, go to **View** > **Welcome Screen**.

5.2.2. Extraction summary tab

The **Extraction Summary** tab is displayed automatically whenever you open a new extraction for analysis.



The Extraction Summary tab has the following sub tabs:

- **All Content:** Includes information on the extractions, device information and device content. For more information, see All Content tab (below).
- **Extractions:** A tab for each type of extraction performed. See Extraction tabs (on page 104).

5.2.2.1. All Content tab

The All Content tab includes the following information:

Extractions (on the facing page)

Case Information (on page 100)

Device Info (on page 101)

Device Content (on page 102)

5.2.2.1.1. Extractions

This section includes information related to the device extractions.

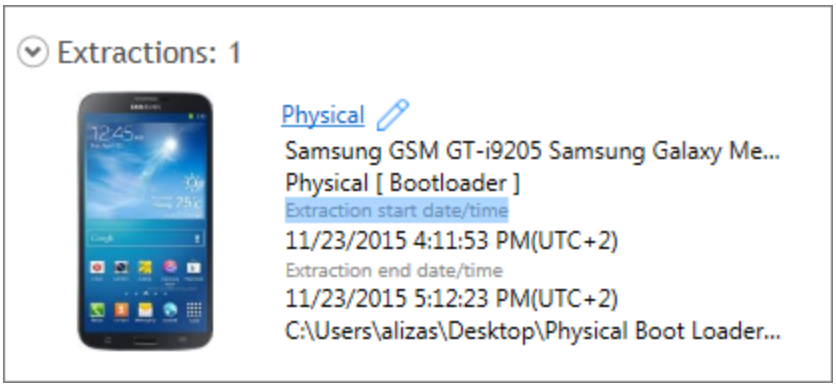


Figure: *Single extraction*

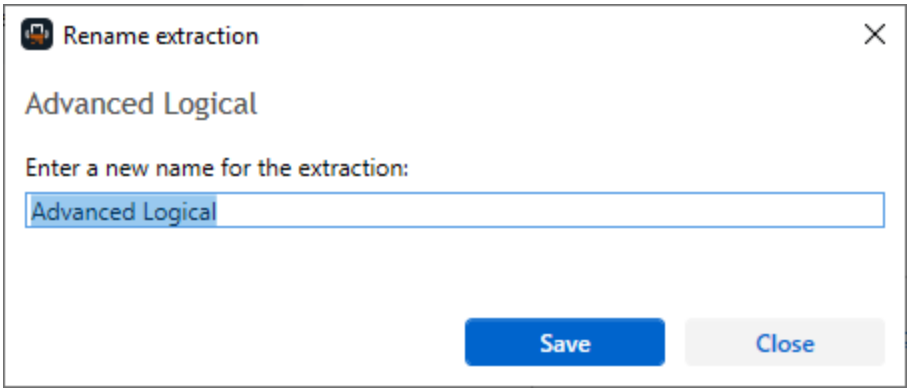
Figure: *Project with multiple extractions*

The Extractions area includes the following information:

Extraction link	Link to the extraction tab.
Device model	Detected model e.g., MB717, Samsung GT-I9205.
Type of extraction	Type of extraction performed e.g., Physical (Bootloader).
Extraction start date/time *Extraction end date/time*	When the extraction started and ended.
Path to the extraction file	The location of the extraction file.

To rename an extraction:

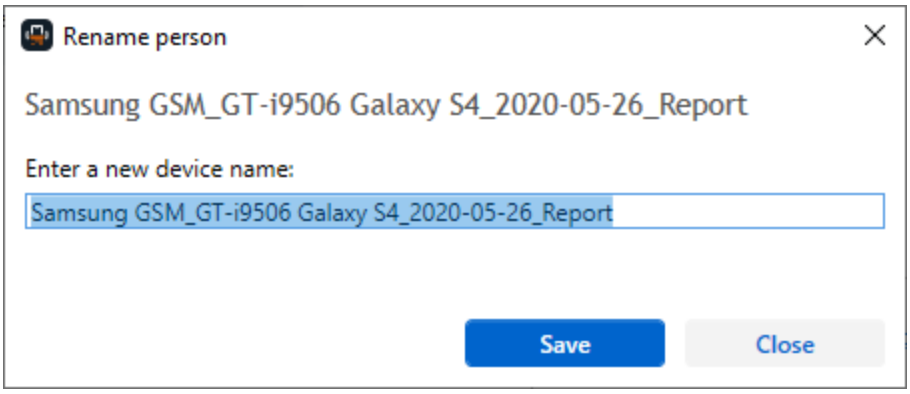
1. Click the Edit button ( ) or select the extraction name in the project tree, right-click and then select **Rename**. The following window appears.



2. Enter a new name for the extraction and then click **Save**.

To rename a project:

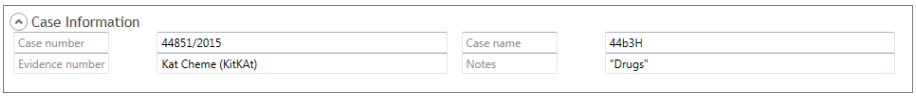
1. Select the project name in the project tree.
2. Right-click and then select **Rename**. The following window appears.



3. Enter the required name for the project.
4. Click **Save**.

5.2.2.1.2. Case Information

This section includes the case information, which is taken from the **Project settings** > **Case Information**.



5.2.2.1.3. Device Info

This section displays a summary of the specific device information taken from the extraction file.

The following example shows device information for a project with multiple extractions.

Device Info

Logical

Detected manufacturer	samsung	Information from XML
Detected model	GT-I9205	Information from XML
Phone revision	4.4.2 KOT49H I9205XXU	Information from XML
IMEI	357426050266879	Information from XML
Phone date/time	11/23/2015 3:54:03 PM	Information from XML
Client Used for Extraction	Yes	Information from XML
Extraction Notes		
Generic	+ZZ – Extracted phone Last IMEI digit might be	Information from XML

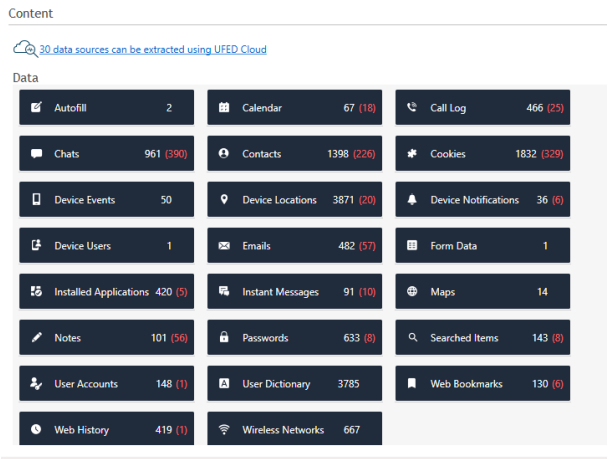
Physical

Android ID	5236fef524a49eea	settings.db-wal : 0xA9...
Bluetooth MAC Address	BC:72:B1:54:36:EA	settings.db-wal : 0xAF...
Bluetooth device name	Galaxy Mega	settings.db-wal : 0xAF...
OS Version	4.4.2	build.prop : 0xED
Detected Phone Model	GT-I9205	build.prop : 0x1A3
Android fingerprint	samsung/meliusltexx/m	build.prop : 0x3C5
Detected Phone Vendor	samsung	build.prop : 0x1BD
Mac Address	BC:72:B1:54:36:EB	.mac.info : 0x0
ICCID		
IMSI	425010776252947	com.android.phone_p...
ICCID	899720203585963501	CheckinService.xml : 0...
IMSI	425020358596350	CheckinService.xml : 0...
Phone Activation Time	6/1/2015 1:34:21 PM(U	
Factory number	RF1D575GRBB	serial_no : 0x0
Locale language	en	persist.sys.language :...
Country Name	US	persist.sys.country : 0x0
Time Zone	Asia/Jerusalem	persist.sys.timezone :...
IMEI	357426050266879	2400257.cfg : 0x100
Mock locations allowed	False	com.android.settings_...
Auto Time Zone	True	com.android.settings_...
Auto Time	False	com.android.settings_...

5.2.2.1.4. Device Content

This section includes the analyzed content, which is divided into the following categories:

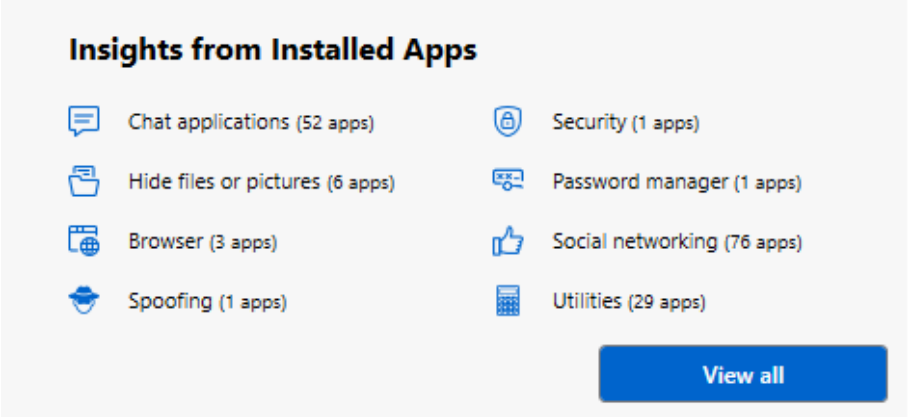
- **Phone Data:** The types of analyzed device data found in the extraction, such as call logs, contacts, instant messages, and so on. For the complete list of phone data types, see Analyzed data (on page 89)
- **Data Files**: The types of standard data files found in the extraction, such as applications, audio, configurations, images, videos, text files, and uncategorized. See Data files (on page 429).
- **Camera Evidence:** Pictures or videos of a device. See Camera and screenshot evidence (on page 403).
- **Phone Evidence:** Screenshots of the device. See Camera and screenshot evidence (on page 403).



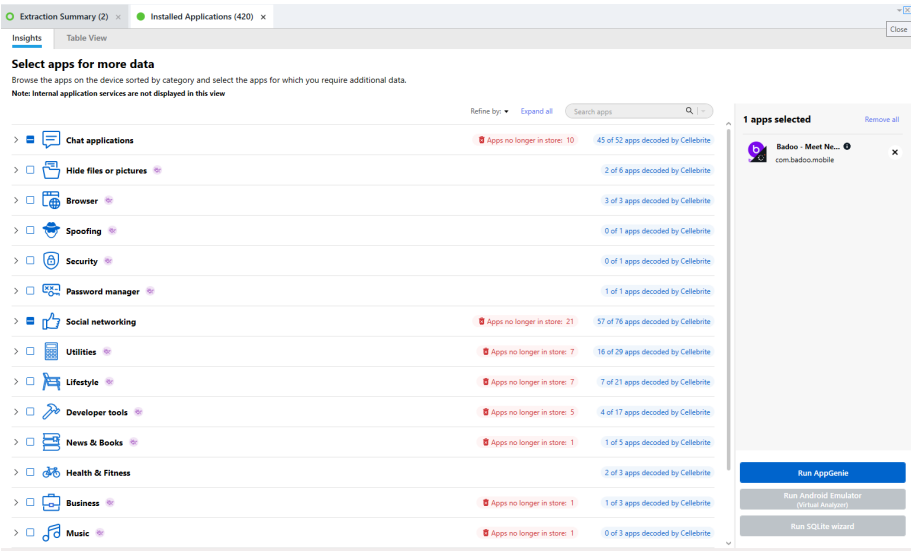
> The number in white indicates the total number of items, and the number in red (in parenthesis) indicates that the item was found in deleted data.

5.2.2.1.5. Insights from installed apps

Insights from installed apps allows the user to get a peek into the types of apps installed on the device. This areas displays app categories and the number of apps in each.

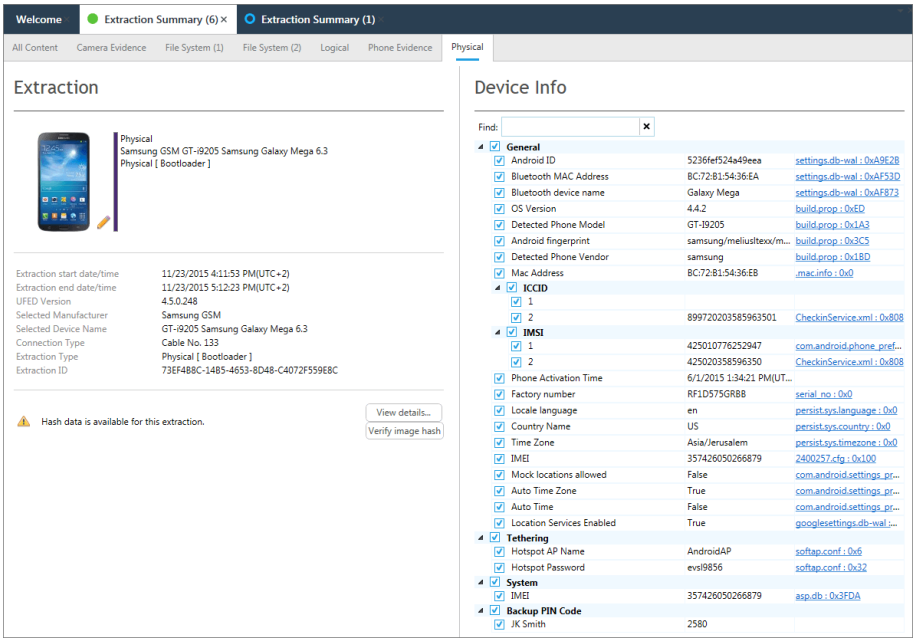


Click to **View all** to open the Insights tab.



5.2.2.2. Extraction tabs

An extraction tab is displayed for each type of extraction. The extraction tabs display extraction information such as when the extraction was performed, by what Cellebrite UFED unit, using which cable as well as Image Hash Information, which is used for the verification of the logged hash values of the parsed images. See Verifying hash values (on page 364). In each extraction tab you can use the find box to search for device specific information.



Extraction information includes the following:

Extraction start date/time *Extraction end date/time*	When the extraction started and ended.
Unit Identifier	The serial number of the device that performed the extraction (e.g., Cellebrite UFED Touch), or a unique ID if the extraction was performed by a PC application (e.g., Cellebrite UFED 4PC).
Unit Version	Cellebrite UFED software version (e.g., 4.1.0.220)
Selected Manufacturer	Manufacturer of the device (e.g., Apple)
Selected Device Name	Device name (e.g., iPhone 4)
Connection Type	Cable used for the extraction (e.g., Cable No. 100)
Extraction Type	Type of extraction performed (e.g., File system)
Extraction ID	Unique ID for each extraction type
Extraction (UFD) file data integrity	Corruption check status (e.g., Intact, Corrupt, Not Available)

To display the relevant information in a new tab in the data display area, click any of the tree items.

Protecting UFD and Extractions

To enhance protection of extraction files, an implemented corruption check mechanism prevents data loss in transit and manual tempering of extractions. In the extraction summary you can view one of the following corruption check statuses:

- **Intact** - in case the check succeeded.
- **Corrupt** - in case the check fails.

A status of "Not Available" will appear for extractions made with previous versions of Physical Analyzer.

5.2.3. Data tabs

Data tabs show files of a specific type (such as call log, contacts, instant messages, and so on).

Each type of data file has several data display modes:

Application files	Hex View and File Info
Image files	Hex View, Image View, File Info, and Gallery view
Video files	Hex View, File Info, Video View, and Gallery view.
Audio files	Hex View and File Info
Text files	Hex View and File Info
Document files	Hex View and File Info
Databases	Database View, Hex View and File Info
Configurations	Hex View and File Info

Data tabs display the data in a variety of sub-tabs, depending on the data type:

- Table view - A list of all the files of a specific type (images, videos, audio, text, and so on) that were found during the data analysis process.
- Folder view - View the folder structure of the data files paths in the reconstructed file system (for data files only).
- Hex view - View the Hex data of a binary item. See Hex view (on page 116).
- Image view - View the image. See Viewing image files (on page 124).
- Thumbnail view - View images by thumbnail (for images only).
- File format viewer - Displays tree-based formats such as: Plist, Bplist, JSON, etc. See File format viewer (on page 120).
- File Info - View information about the file. See File Info tab (on page 120).
- Database view - View the contents of database files. See Database view (on page 112).
- Gallery view - View images and videos in Gallery format.

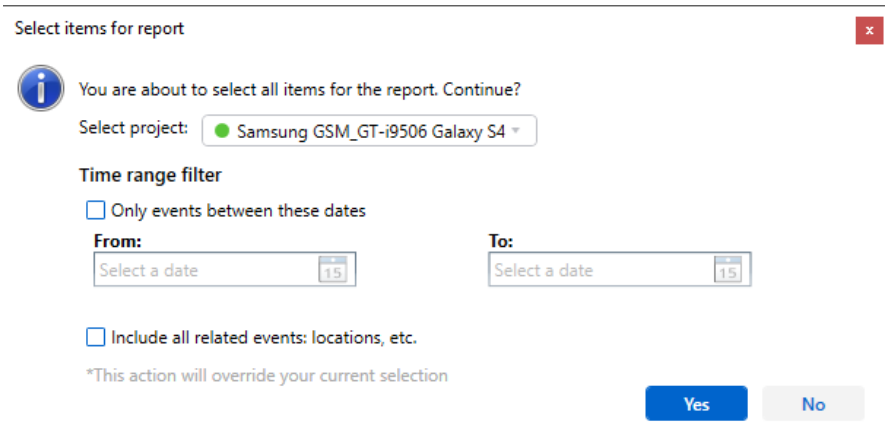
5.2.3.1. Working in data tabs

Selecting items

Select items in the data display area to include them in any report you generate. By default, all items are selected.

- To select multiple items, hold the SHIFT or CTRL keys (consecutive and nonconsecutive selection).
- When an item is selected, press the space bar to select or clear the check box, which indicates if the item should be included or excluded from the report.
- To select all items at once, click ✓ in the column header (table view, thumbnail view and timeline).
- To select items and optionally include a timeframe:

1. Click ⋮ and select **Select items for report**.



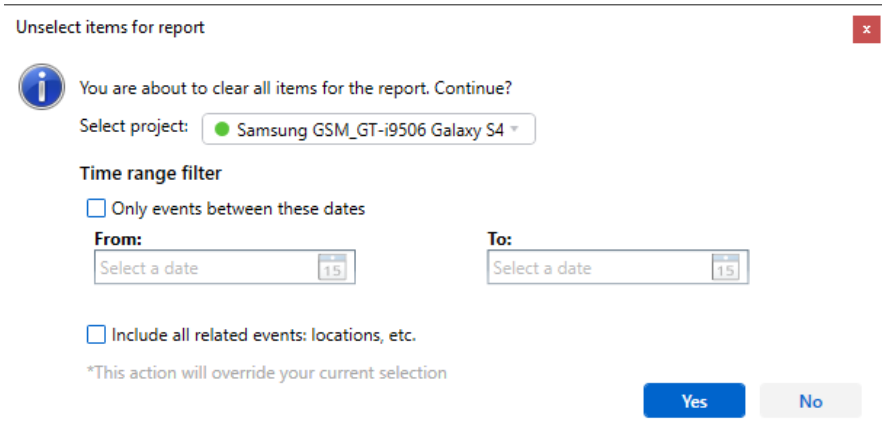
2. To select all click **Yes.**
3. To set a timeframe for selection:
   a. Check **Only events between these dates**.
   b. Select the **From** and **To** dates.
   c. Click **Yes**.

> To include related events select **Include all related events: locations, etc**. This action overrides the current selection.

Unselecting items

Unselect items in the data display area to exclude them from any report you generate.

» To unselect all items at once, click — in the column header (table view, thumbnail view and timeline).



» To unselect items and optionally include a timeframe:

1. Click ⋮ and select **Unselect items for report**.
2. To unselect all click **Yes.**
3. To set a timeframe to unselect items:
   a. Check **Only events between these dates**.
   b. Select the **From** and **To** dates.
   c. Click **Yes**.

Sorting columns

Sort each column alphabetically or by time.

» Click the column header to toggle the order.

Re-ordering the columns

For your convenience, you can change the order of the columns. Your preference is retained for the duration of the session.

» Drag the desired column to the desired location.

Hide or show columns

» Right-click the column header and select the column name in the list.

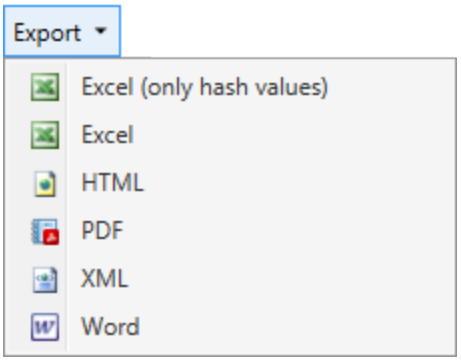
Viewing more information

For data tabs containing textual information, by default the right pane is open, displaying the selected item's information.

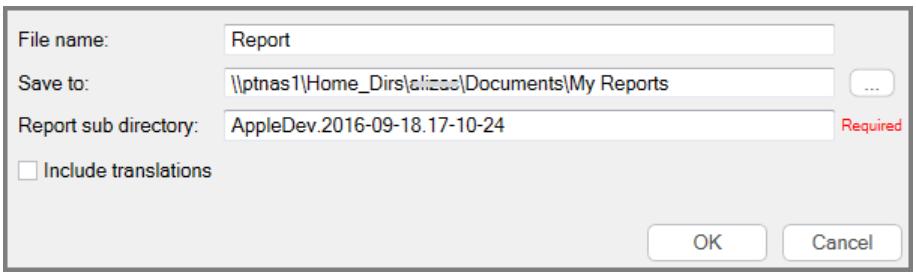
» To close or open the right pane, click .

Exporting data

1. To export the data in a particular tab, click the desired output in the toolbar: Excel, HTML, PDF, XML, KML (location data only), or EML (email data only).



The Export Dialog Window appears.



2. Do one of the following:
   - Enter the path where you want to save the report.
   - Click ... and browse to and select the desired location.
3. Select the **Include translations** check box to include translated data.
4. Click **OK**.

   The report is generated, and a message appears asking if you would like to open it in third party software.
5. Click **Yes** or **No**.

   The file is opened in the default third party software.

> When exporting to EML, a file is created for each email.

5.2.3.2. Table view for data files

For data files, the table shows the following information:

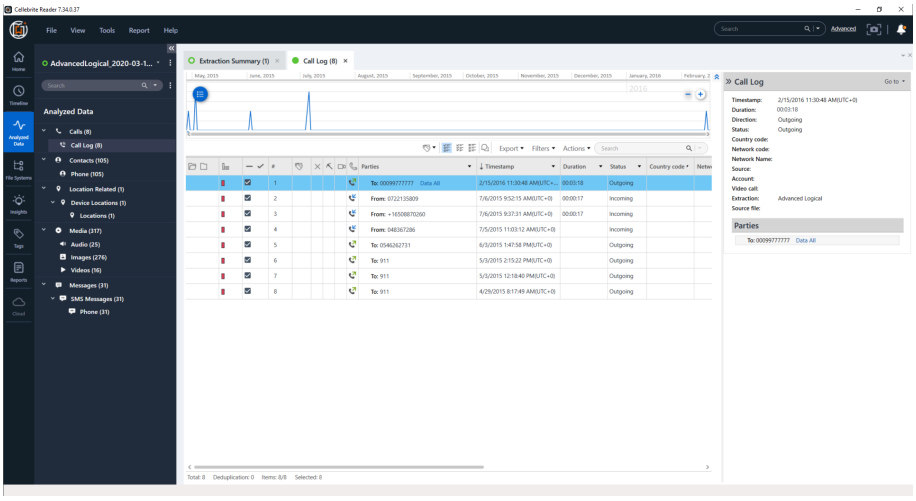
	Indicates whether to include (select) or exclude (clear) the item in the report.
#	Row number.
	Indicates if the item is bookmarked.
	Indicates whether the data file was deleted , or has an unknown status ("?" or white document icon).
	Indicates if the data file includes an attachment.
Image	A thumbnail of the image or an icon of the file type. (Image data files only).
Name	The file name.
Path	The root path of the data file in the file system.
Size	The size of file.
Metadata	Additional metadata of the data file.
Created	The creation time stamp of the data file.
Modified	The modification time stamp of the data file.
Accessed	The last access time stamp of the data file.
Attachment source app	Indicates the source application for the attachment as well as an indication if it was sent or received.
Bookmark Note	Details of the bookmark.

In addition, indicators are displayed to show attachments, indicate video calls, and to show even direction.

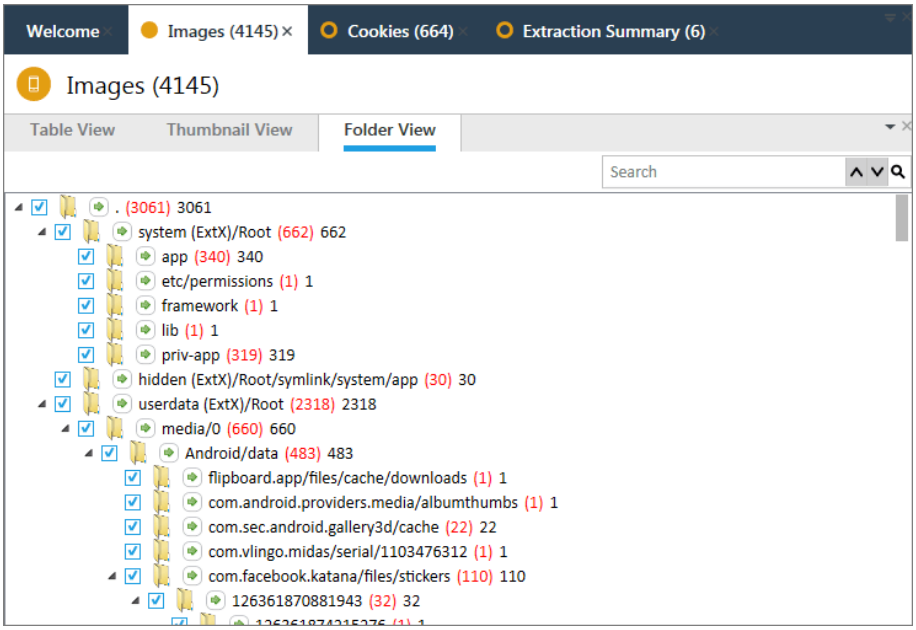
» Double-click on an item record (table row) to open a Hex Viewer tab showing the Hex data of the selected file.

5.2.3.3. Table view for analyzed data

For analyzed data, table view tabs display a list of all the events of a specific type (Call Log, Contacts, Instant messages, and so on) that were found during the data analysis process.



5.2.3.4. Folder view



Folder view shows how the items were organized in the device.

- Select the folder checkbox to select all the items in that folder (including sub-folders). Selected items are included in generated reports. When you select an item, it is selected in all tabs in the data display area.
- Click to open the folder in a new tab in the data display area.

The following folder information is displayed:

- The folder name in the extracted file system.
- The number of selected items in that folder (red in brackets).
- The total number of items in that folder (in black).

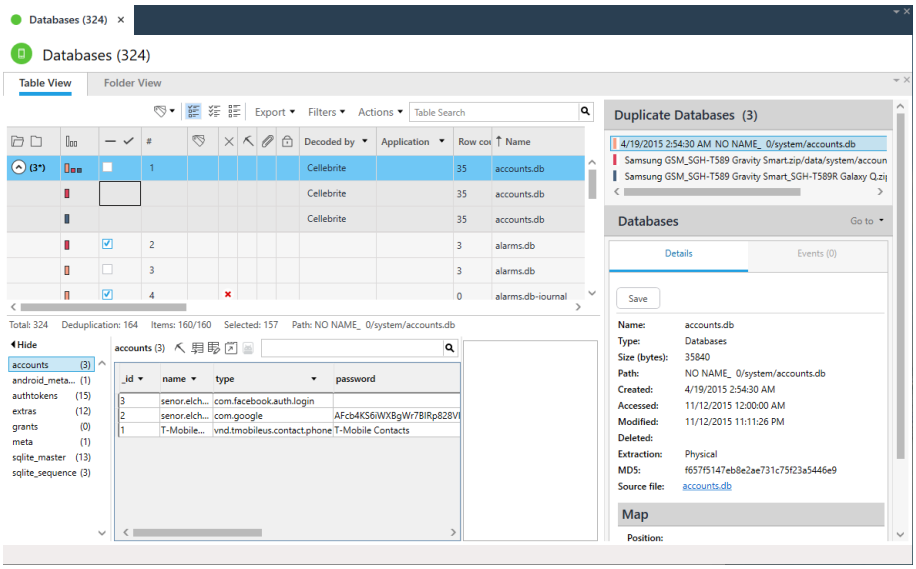
5.2.3.5. Database view

Database view displays the contents of database files that were found in the extraction. It improves your data reviewing capabilities within database content and includes the following capabilities:

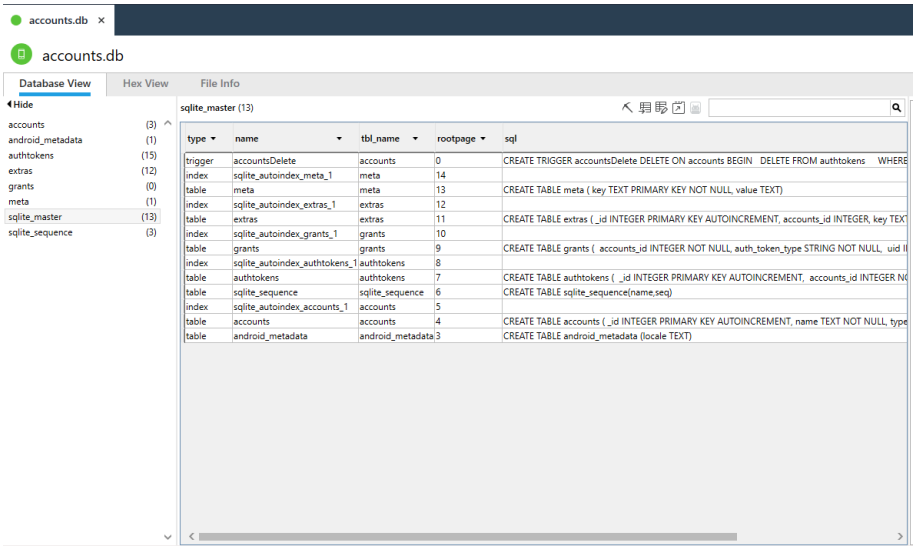
- **Advanced viewing:** Links between database values and their source within the Hex format, making evidence validation and investigation easier and clearer. You can decode data in the database file without the need to copy it or switch to Hex view.
- **Auto-detect cell content type and cell selection:** Converts timestamp to human-readable format, decode base64 data, embedded images preview, file format viewer, etc. It also includes extra decoding capabilities to database values.
- **Deleted data (recovered records):** View deleted database records as well as intact data, making SQLite carved records more accessible and legible.
- **Search:** Enhanced search capabilities.

To open Database view:

1. Double-click the Databases tree item under Data Files. The following window appears.

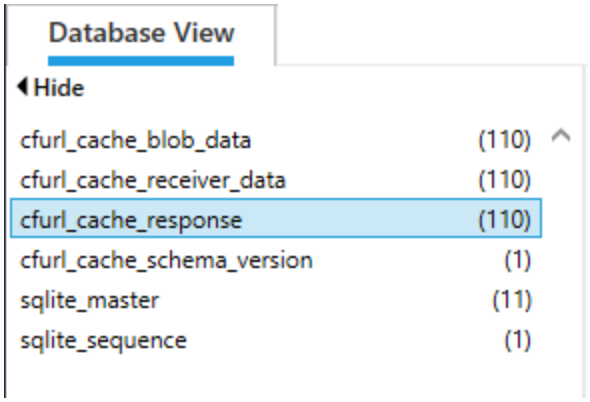


2. Double-click a row to open the Database view.

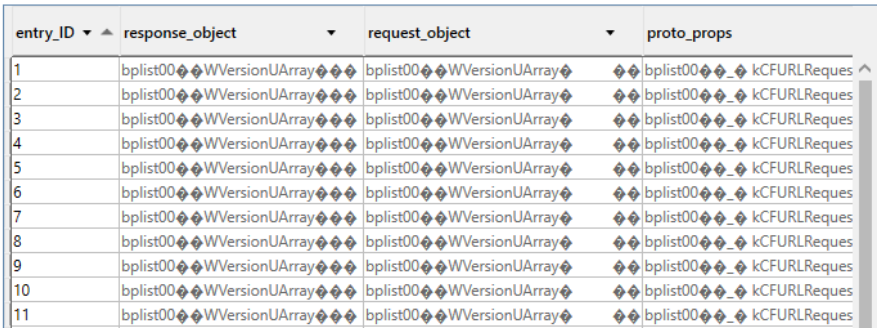


Database view consists of the following sections:

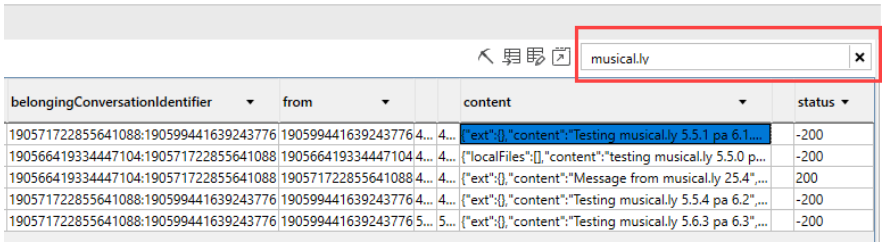
- List of the database tables. The number in parenthesis next to each table name designates the number of records in the database table. Select a table in the left column to display its records.



- Records display areas containing a list of data records in the selected database table.



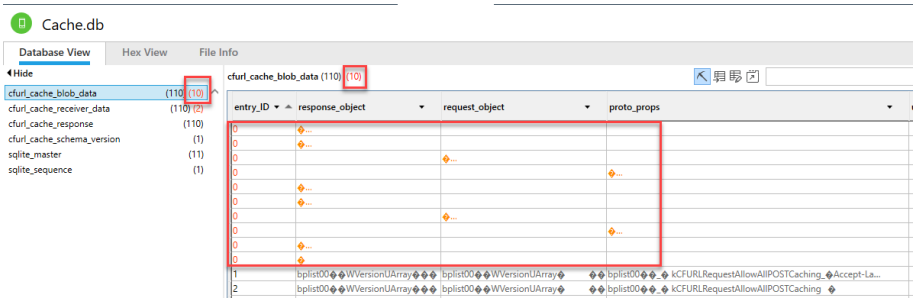
» Search field to filter the displayed records.



» Use the buttons toolbar ( ) to: Include recovered records, export to CSV, open the SQLite wizard or open the Virtual Analyzer.

To include recovered records:

» Click . The recovered records are indicated in red.

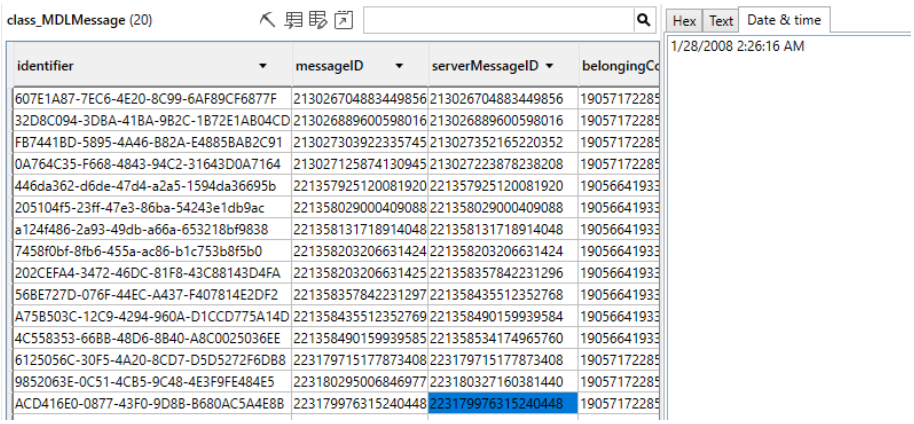


» Select records to auto-detect cell content type and display the data in the right pane. See the examples below.

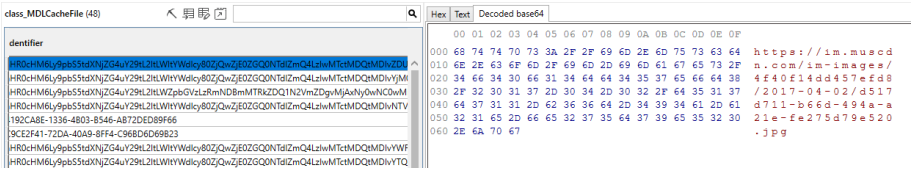
5.2.3.5.1. Examples

The right pane displays a cell's data more clearly in a view for each data-type. Examples are shown next.

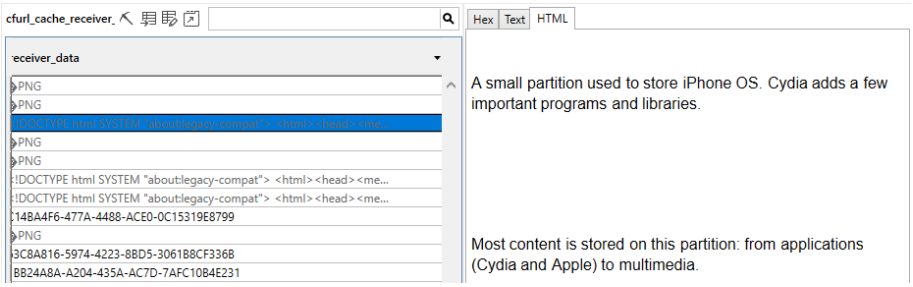
Date and time



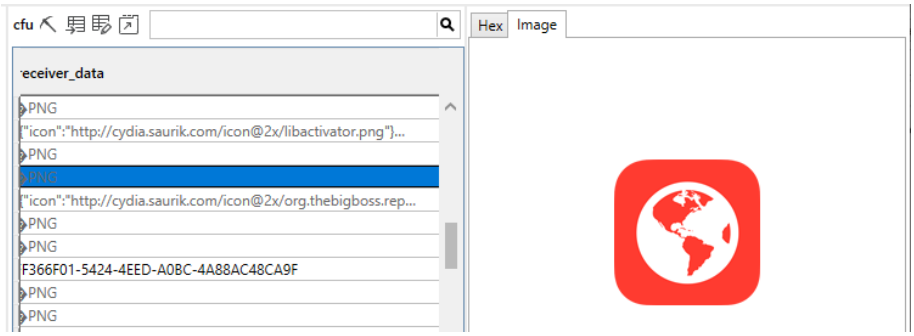
Decode base64



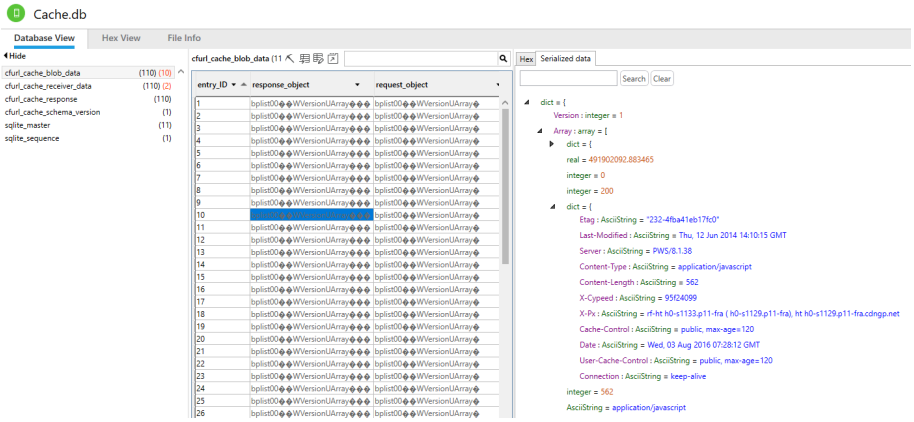
HTML



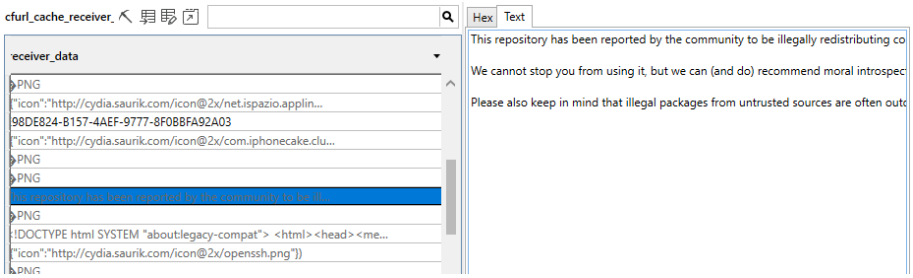
Image



Serialized data

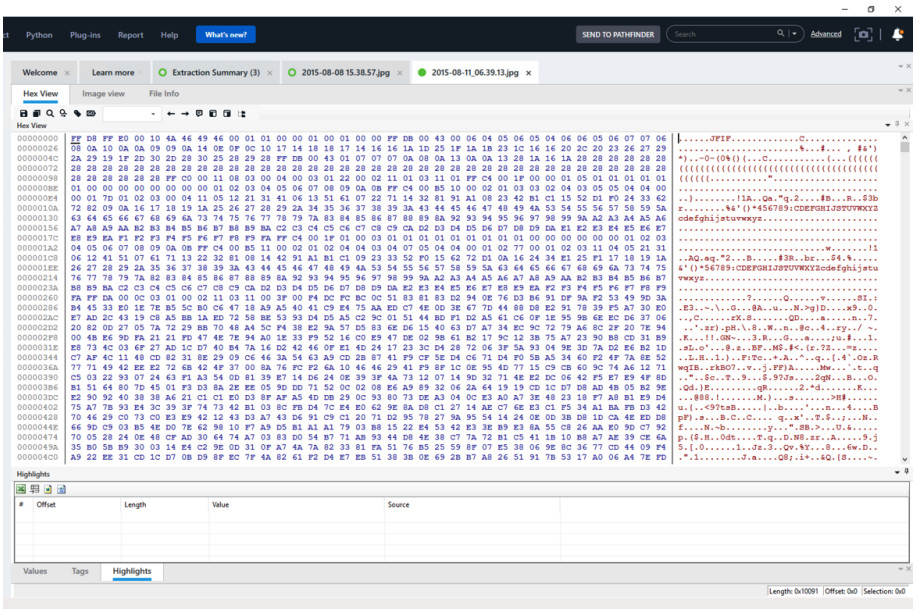


Text



5.2.3.6. Hex view

A Hex view tab appears for each binary item you open from the project tree. When opening, for example, an Image memory disk, a Hex view tab opens alone. When opening a binary item, for example, an image file, the Hex view tab may be accompanied by other tabs.



The Hex view tab contains the following sections:

Hex tabs

- **Address column:** The number of information column in Hex or Decimal value, displaying the start address of each row in the Hex and ASCII representation data sections.
- **Hex data view column:** The Hex data of the selected item.
- **ASCII representation view column:** The ASCII representation of the Hex data.

An information frame automatically appears when you position the mouse over the information displayed in the Hex view. The information frame displays links (pointers) to analyzed data items, such as files and folders in the project tree, and search results associated with the pointed data.

Hex view toolbar

	Save	Click to save the entire memory extraction to a local folder.
	Copy Selection	Copy the currently selected content of the Hex View tab to the clipboard.
	Find	Displays the Find dialog to search for all occurrences of specified information in the displayed Hex display pane.
	Find Next	Displays the Find dialog box with the search parameters used in the latest search.
	Add Tag	Bookmark the currently selected content of the Hex display pane.
	Go To	Redirect the offset to specific address in the content of the Hex display pane.
	Enable Info Frame	Toggles on/off the display of floating information frame at the cursor location.
	Show Address	Toggles on/off the left address column display.
	Show ASCII view	Toggles on/off the right ASCII representation column display
	Locate file in tree	Locate the file in the data tree.

Analysis information tabs

Located under the Hex view tab are Analysis Information tabs that display the following types of information related directly to the displayed Hex data:

- **Values** - A wide array of value interpretations, such as 8, 16, 32, and 64 bit, various string encoding, date & time formats, and more, calculated on the fly for the currently selected data in the Hex view. See Working in the Values tab (below).
- **Tags** - A list of tags added in the displayed Hex data. See Working with Hex tags (on page 398).
- **Highlights** - A list of content segments markups highlighted in the displayed Hex data. The number of highlight results is shown in brackets next to the tab name. See Working in the Highlights tab (on the facing page).
- **Search** - Displays results of a search in the displayed Hex data. A new search results tab opens for each search query performed. The number of results for each search is shown in brackets next to the tab name.

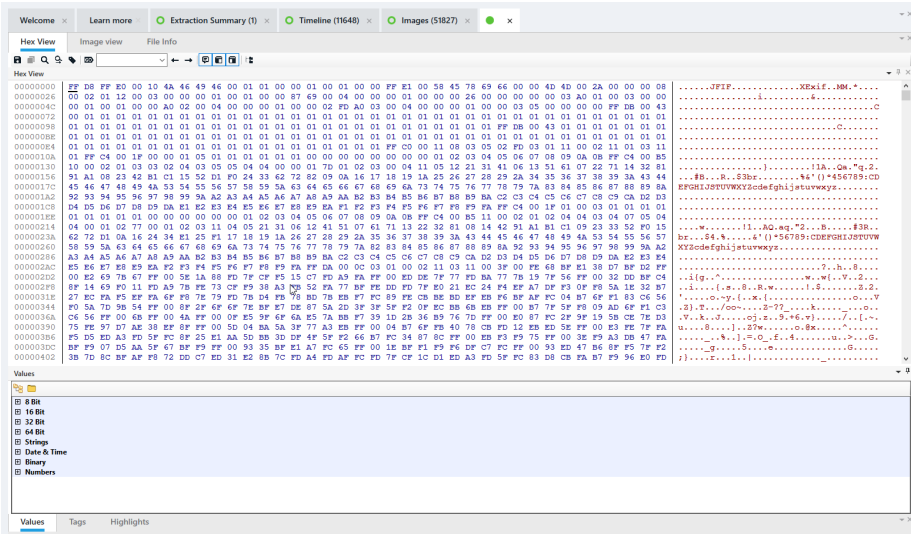
You can rearrange the display of the Analysis Information tabs to suit your preference:

- Double-click the header strip of the section to display the entire section as a floating panel. Double click the floating panel header strip to dock it back to the default location (at the bottom of the Hex View tab).
- Double click the name label of any tab to display it as a floating panel. Double click the floating panel header strip to dock it back to the original location.
- Drag the name label or floating panel over any of the docking labels that appear to dock it at that location in the Hex View tab.

5.2.3.6.1. Working in the Values tab

Decode the raw data to a variety of encoding types in real time, and expand them in the Values list.

1. To access the **Values** tab, click the **Values** tab at the bottom of a **Hex view** tab.



2. Select a data segment in the Hex.
3. To display the decoded data, scroll to the desired encoding, and click ⊞ to expand the display.

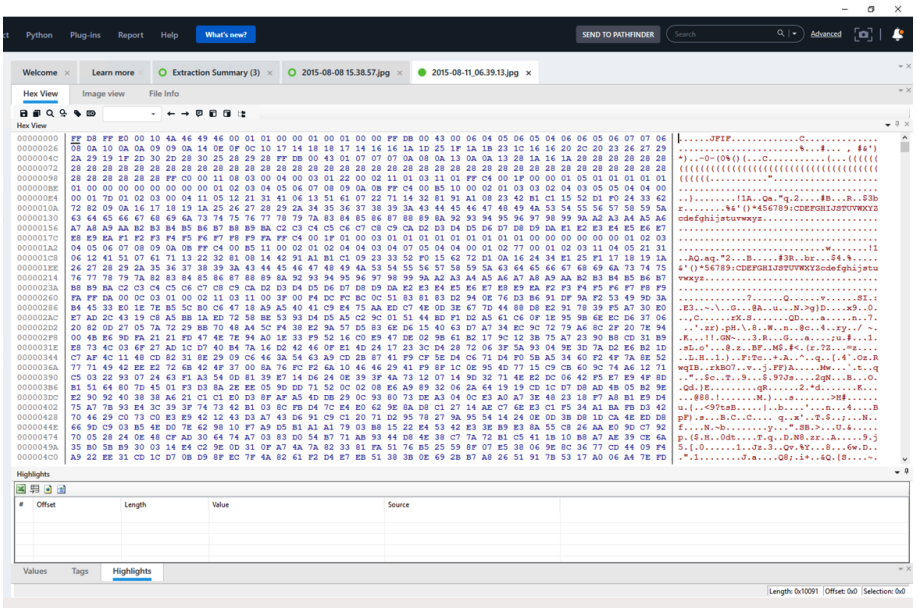
   Some encoding options, such as 16 Bit, have sub-encoding types.

4. Fully expand or collapse all encoding types by clicking or .

5.2.3.6.2. Working in the Highlights tab

The **Highlights** tab contains a list of content segments that are highlighted in the displayed Hex data. Each segment represents locations of analyzed data within the Hex. The **Highlights** tab enables you to locate particular types of analyzed data in the Hex. The number of highlight results is shown in brackets next to the tab name.

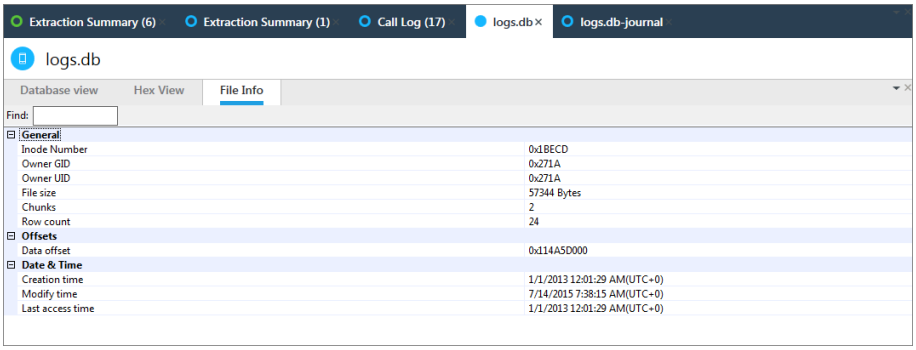
1. To access the **Highlights** tab, click the **Highlights** tab at the bottom of a **Hex view** tab.



2. In the project tree, click an **Analyzed Data** folder (for example, **Contacts**).

   The location of the selected folder is highlighted in the **Hex view** tab, and the list of chunks that the folder is comprised of is listed in the **Highlights** tab.

5.2.3.7. File Info tab



The File Info tab displays the following information about the data file:

- **FAT** – The File Allocation Table of the extended attributes.
- **Date & Time** - Created, Modified, and Last Access time stamps of the data file.
- **General** - The file size in bytes and the number of file system chunks of which the data file is comprised.
- **Offsets** - The offset addresses of the data file in the Hex data.
- **EXIF** - The embedded EXIF information logged by the camera (if it exists).
- **File Metadata** - The general information of the image (capture time, resolution, size and color depth).

5.2.3.8. File format viewer

A file viewer that displays tree-based (hierarchical) formats. It supports the following data formats: Property list (Plist), Binary property list (Bplist), JSON, Serialized Java object, MessagePack, and SharedPreferences.

An example is displayed next.

device_values.plist ×

device_values.plist

File format viewer | Hex View | File format viewer | File Info

Search | Clear

Search results : 0

dict = {

ActivationPublicKey : data = 2D 2D 2D 2D 2D 2D 42 45 47 49 4E 20 52 53 41 20 50 55 42 4C 49 43 20 4B 45 59 2D 2D 2D 2D 2D 0A 4D 49 47 4A 41 6F 47 42 41 4B 77 65 3
62 6E 4F 37 56 6A 5A 6E 57 79 43 41 4C 55 6C 0D 0A 75 67 43 6F 66 6A 76 6E 2F 46 4C 79 53 62 63 62 79 4E 36 33 44 5A 61 43 31 46 51 6A 2F 6D 6D 32 6B 73 31 5A 7
79 6D 52 67 69 31 64 76 4E 6E 35 59 54 56 37 68 58 69 7A 6A 77 63 55 2F 4C 35 53 4B 67 4D 6D 53 6D 37 6A 58 7A 49 42 57 63 62 32 67 42 41 67 4D 42 41 41 45 3D 0

ActivationState : string = Activated

ActivationStateAcknowledged : true = True

BasebandSerialNumber : data = 11 56 F8 BB

BasebandStatus : string = BBInfoAvailable

BasebandVersion : string = 4.52.00

BluetoothAddress : string = a0:99:9b:53:9b:b0

BuildVersion : string = 13C75

CPUArchitecture : string = arm64

DeviceCertificate : data = 2D 2D 2D 2D 2D 2D 42 45 47 49 4E 20 43 45 52 54 49 46 49 43 41 54 45 2D 2D 2D 2D 2D 0A 4D 49 49 43 38 7A 43 43 41 6C 79 67 41 77 49 42 4
44 42 61 4D 51 73 77 43 51 59 44 0D 0A 56 51 51 47 45 77 4A 56 55 7A 45 54 4D 42 45 47 41 31 55 45 43 68 4D 4B 51 58 42 77 62 47 55 67 53 57 35 6A 4C 6A 45 56 4
44 56 51 51 44 45 78 5A 42 63 48 42 73 5A 53 42 70 55 47 68 76 62 6D 55 67 52 47 56 32 61 57 4E 6C 49 45 4E 42 4D 42 34 58 44 54 45 31 4D 44 67 78 4D 44 49 7A 0
41 72 42 67 4E 56 42 41 4D 57 4A 44 49 31 51 54 6B 35 51 6A 41 79 4C 54 4D 34 4E 44 67 74 0D 0A 4E 44 51 30 52 69 31 42 52 6B 45 78 4C 55 45 30 51 6A 41 35 4D 6
67 54 41 6B 4E 42 0D 0A 4D 52 49 77 45 41 59 44 56 51 51 48 45 77 6C 44 64 58 42 6C 63 6E 52 70 62 6D 38 78 45 7A 41 52 42 67 4E 56 42 41 6F 54 43 6B 46 77 63 47
6E 7A 41 4E 42 67 6B 71 68 68 69 47 39 77 30 42 41 51 45 46 41 41 4F 42 6A 51 41 77 67 59 6B 43 67 59 45 41 72 42 37 78 6A 6F 4A 65 44 52 6F 79 0D 0A 2F 4B 38 79
53 57 36 41 4B 68 2B 4F 2B 66 38 55 76 4A 4A 74 78 76 49 33 72 63 4E 0D 0A 6C 6F 4C 55 56 43 50 2B 61 62 61 53 7A 56 6E 49 44 35 51 6B 45 6D 42 35 48 6F 65 68 39
0A 75 46 65 4C 4F 50 42 78 54 38 76 6C 49 71 41 79 5A 4B 62 75 4E 66 4D 67 46 5A 78 76 61 41 45 43 41 77 45 41 41 61 4F 42 6C 54 43 42 6B 6A 41 66 42 67 4E 56 48
64 44 41 64 42 67 4E 56 48 51 34 45 46 67 51 55 47 36 59 63 52 43 6A 42 70 74 72 53 4B 51 2F 5A 6F 74 48 69 53 6A 64 75 0D 0A 57 58 77 77 44 41 59 44 56 52 30 54
52 30 6C 41 51 48 2F 42 42 59 77 46 41 59 49 0D 0A 4B 77 59 42 42 51 55 48 41 77 45 47 43 43 73 47 41 51 55 46 42 77 4D 43 4D 42 41 47 43 69 71 47 53 49 62 33 59
41 50 42 43 77 58 6A 48 38 4A 77 43 6A 36 58 6D 35 69 2F 35 32 59 4B 6C 70 50 59 32 56 74 6D 77 37 6B 4A 4B 49 61 47 49 4F 71 57 7A 74 6E 38 2F 56 76 4D 48 77 6
55 75 35 50 44 45 53 47 35 64 32 66 42 69 56 77 7A 79 30 6C 56 4D 2B 58 69 5A 2B 48 50 68 4F 39 0D 0A 48 71 62 51 33 63 57 4E 7A 67 32 78 69 47 79 38 31 59 4C 4
2D 2D 45 4E 44 20 43 45 52 54 49 46 49 43 41 54 45 2D 2D 2D 2D 2D 0A

DeviceClass : string = iPhone

DeviceColor : string = #e1e4e3

DeviceName : string = shirleym's iPhone

DevicePublicKey : data = 2D 2D 2D 2D 2D 2D 42 45 47 49 4E 20 52 53 41 20 50 55 42 4C 49 43 20 4B 45 59 2D 2D 2D 2D 2D 0A 4D 49 49 42 43 67 4B 43 41 51 45 41 7A 4
30 56 55 68 34 36 36 48 74 47 5A 4E 36 0D 0A 58 72 53 6E 4D 7A 30 74 4A 49 4A 4B 67 57 30 67 79 6D 64 78 48 71 46 79 59 45 31 59 42 30 76 35 49 72 66 5A 4D 43 6
70 2B 71 68 46 78 37 37 76 31 52 38 7A 41 74 57 54 55 4E 67 48 6D 43 64 48 48 71 41 52 78 65 39 62 4C 38 2F 75 58 31 68 33 6D 66 62 49 6E 32 4A 78 5A 41 48 70 55
42 71 41 79 41 4A 4F 66 76 55 70 55 34 46 53 59 49 2B 2B 6F 67 68 56 49 78 77 33 34 38 67 6B 0D 0A 63 72 6A 64 37 32 67 69 6E 52 34 36 31 69 79 54 4C 32 6A 6F 45
32 54 50 7A 7A 78 0D 0A 41 31 34 74 5A 79 32 76 4D 58 37 44 54 61 42 4C 36 37 74 37 64 6F 30 6B 33 75 41 54 2F 2B 42 48 46 77 49 44 41 51 41 42 0A 2D 2D 2D 2D 2

DieID : integer = 357552343476262

FirmwareVersion : string = iBoot-2817.20.26

HardwareModel : string = N61AP

HardwarePlatform : string = t7000

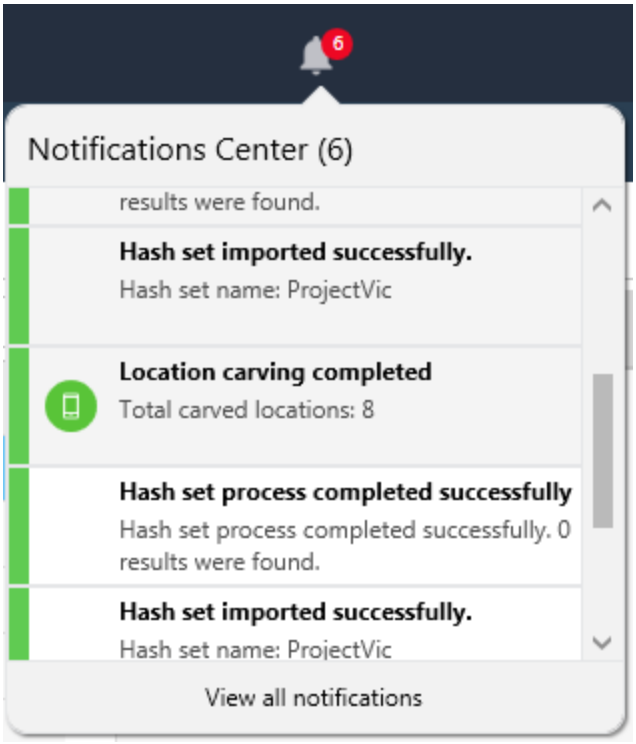
HostAttached : true = True

5.2.4. Notifications center

The Notification center provides improved messaging to enable you to work seamlessness with notifications that keep you up to date with new features and capabilities of Physical Analyzer so you will never miss a thing. In the Notification Center, you can view the latest alerts, news, warnings, and completed actions.

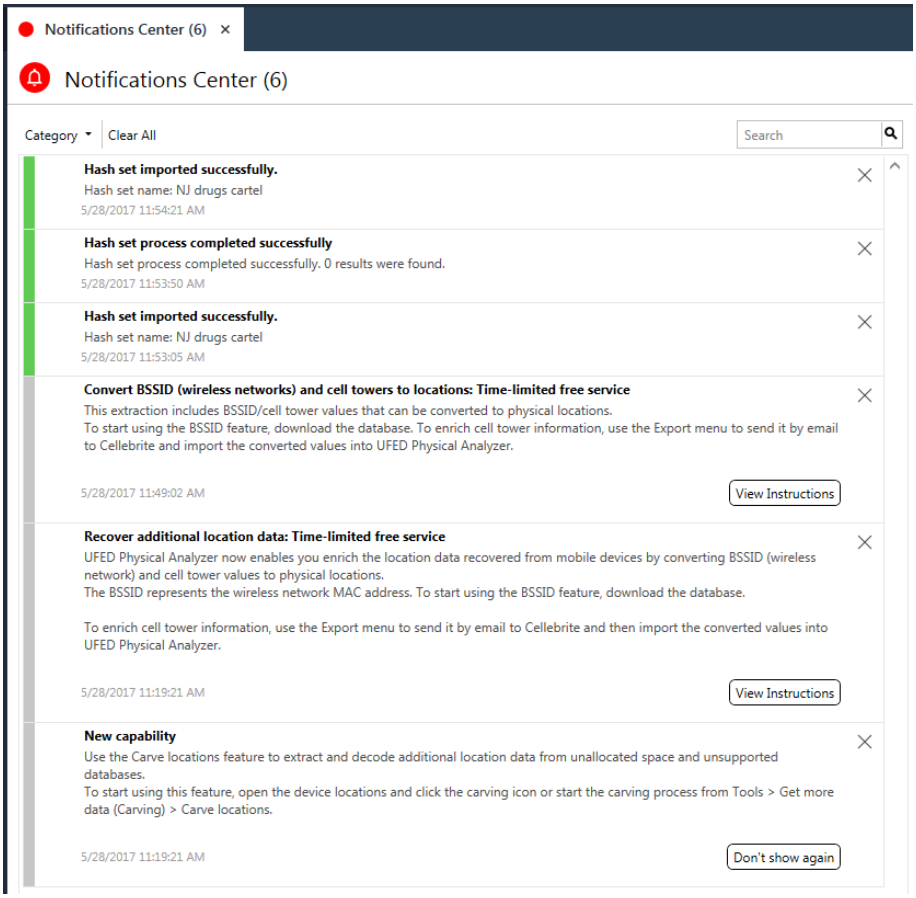
To see your notifications.

1. Click Notifications ( ) on the top right. The following window appears.



> The notification counter resets to zero after the messages have been reviewed.

2. To open the Notifications center, click **View all notifications**. The following window appears.

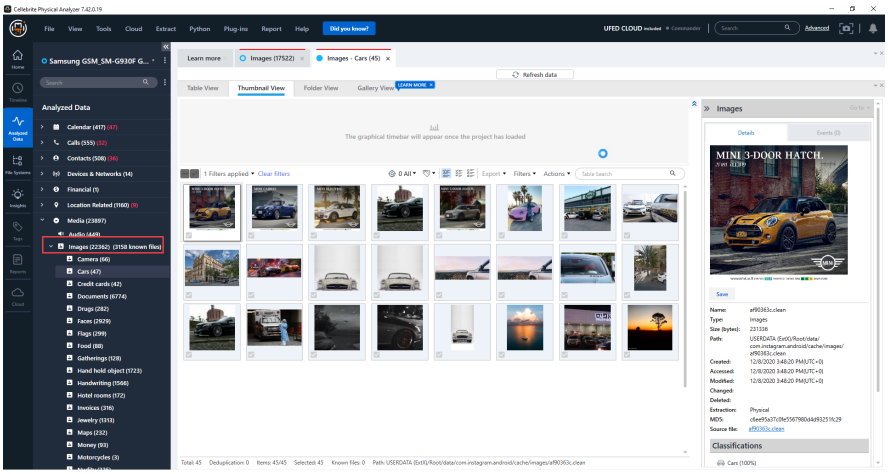


From this window, you can select the message category type to display, that is: Error, Information, Success, or Warning. You can also clear all the existing messages, search for a particular message, view details about the message, and hide messages.

5.3. Viewing image files

1. In the Analyzed data tab, go to **Media > Images**.
2. Double click on Images to open the Images tab.

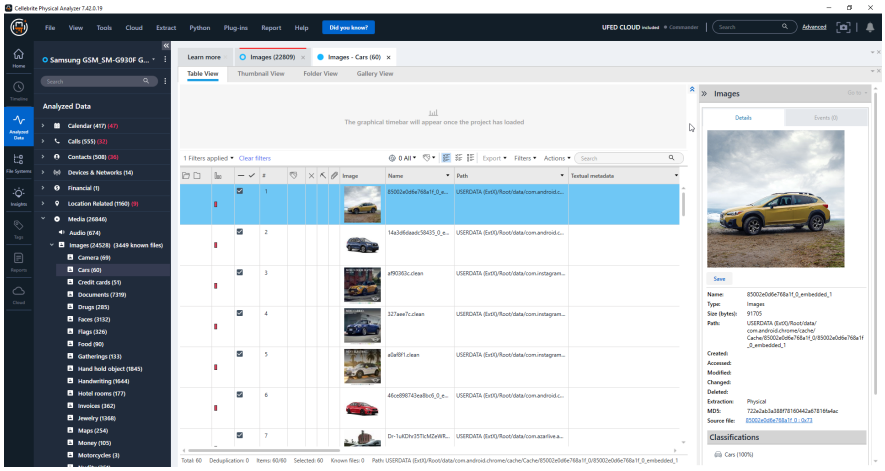
> If media classification was run on the extraction, you can double click the relevant category to open its tab. See Media classification (on page 346).



In the Images tab, you can select the view you wish to see the images. Available views include:

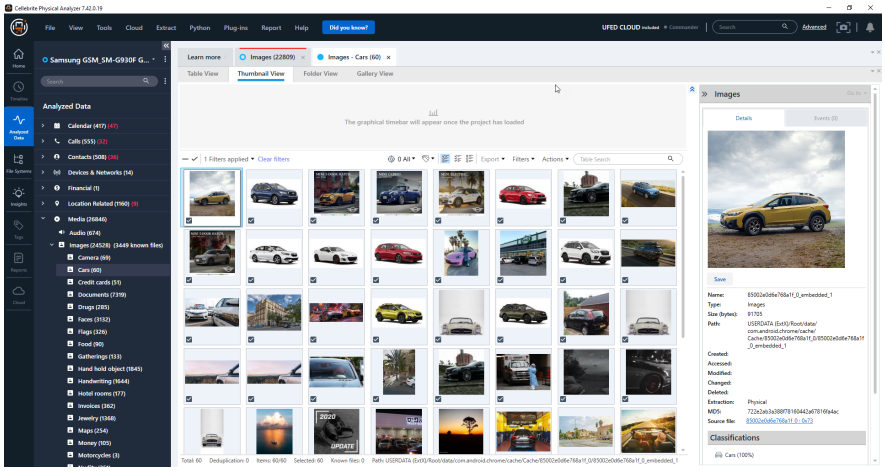
Table view

View a list of all images in table format. Double click on an image to open in a separate tab.



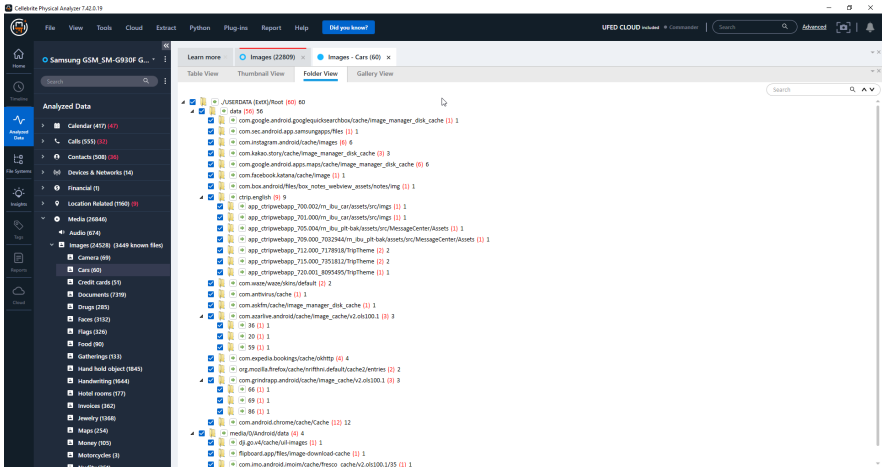
Thumbnail view

View images by thumbnail. Double click the image to open in Gallery view.



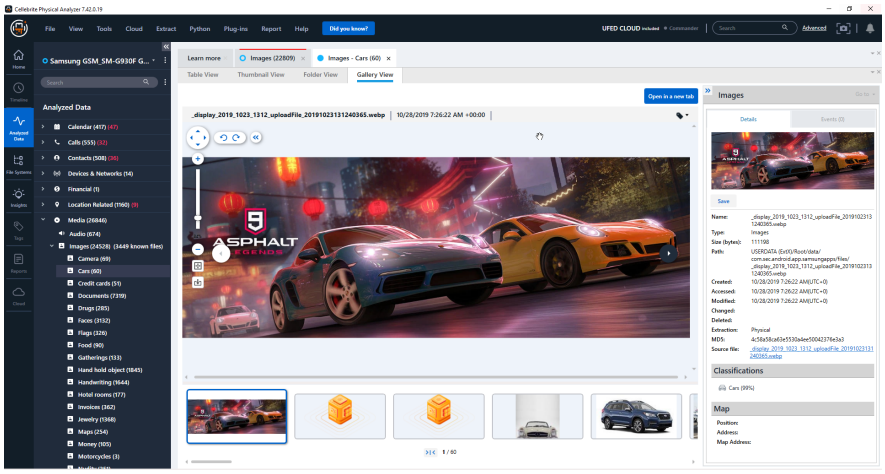
Folder view

View the folder structure of the data files paths in the reconstructed file system. Double click an item to open in Gallery view.



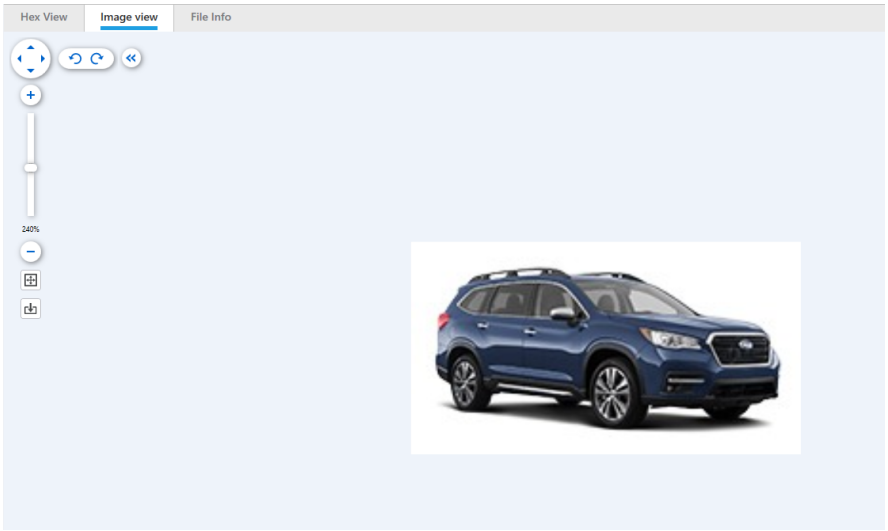
Gallery view

View images in gallery format, easily scrolling through images.



Viewing single images

1. In Gallery view, click **Open in a new tab** to view the image in a seperate tab.



The sub tabs for each image include:

- **Hex view** - view hex data for the image.
- **File info** - view the file information. For example, the File metadata section includes information such as the Capture Time, which is the date and time a photo was taken.
- **Image view** - Use the image controls as needed.

When the image is enlarged, click to navigate the image.

Rotate image clockwise and anti-clockwise.

Zoom in and out. You can also adjust the zoom using the slider.

Zoom to fit the tab.

Reset the zoom to 100%.

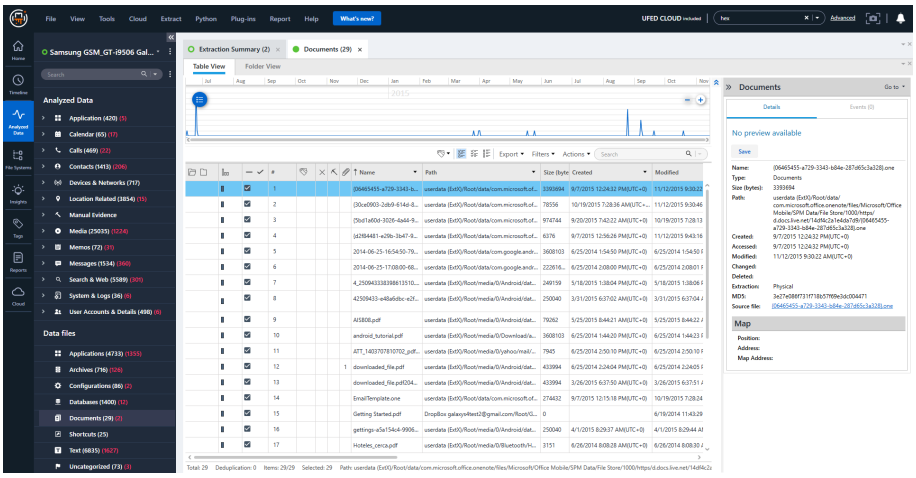
Hide image controls.

5.4. Viewing docs in Physical Analyzer

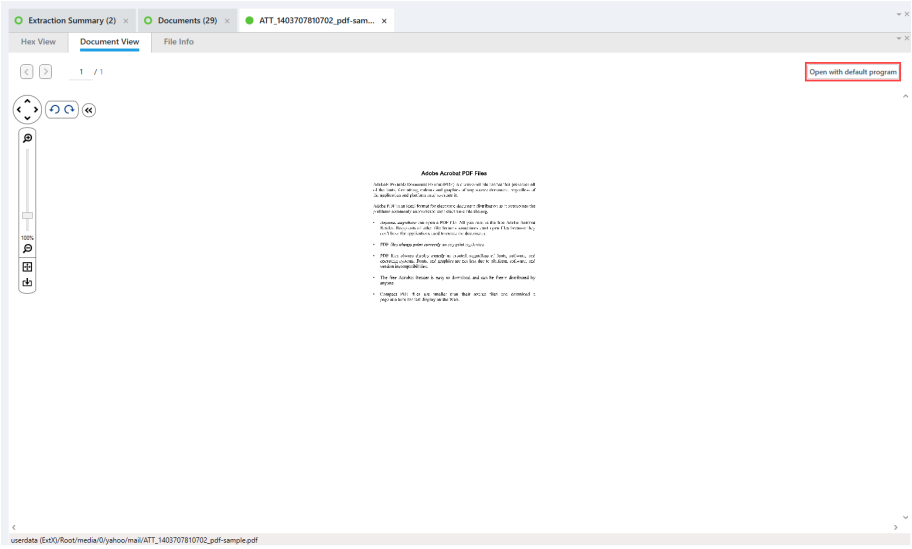
To help optimize the review process, you can view all PDF and Microsoft Office files extracted from a device (Word, Excel and PowerPoint) in Physical Analyzer. If required you can also choose to open the file with the default application.

For a quick view of PDF and Microsoft Office files:

1. Go to Analyzed data view and click **Documents** from the project tree.
2. From the Documents tab, double-click a file to view it.



The following window appears.



To move between the next or previous pages of the file.

When the image is enlarged, click to navigate the image.

Rotate image clockwise and anti-clockwise.

Zoom in and out. You can also adjust the zoom using the slider.

Zoom to fit the tab.

Reset the zoom to 100%.

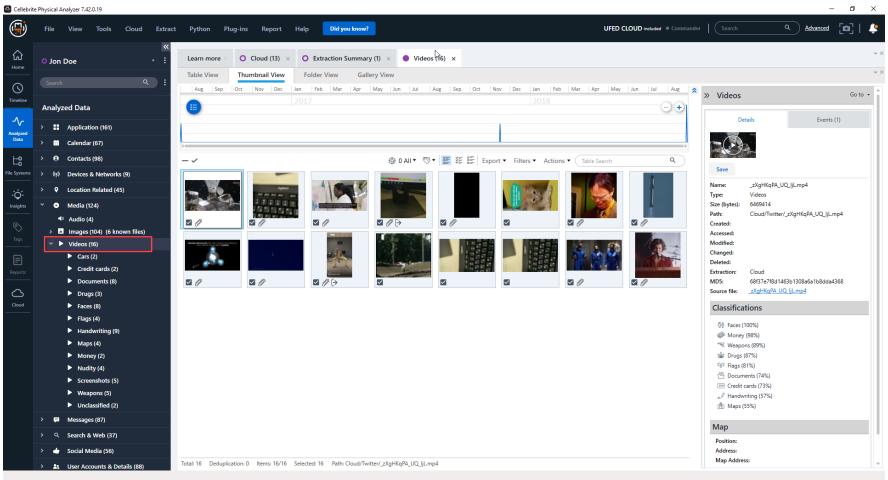
Hide image controls.

To open the file in another application, click **Open with default program**.

5.5. Viewing video files

1. In the Analyzed data tab, go to **Media > Videos**.
2. Double click on Videos to open the Videos tab.

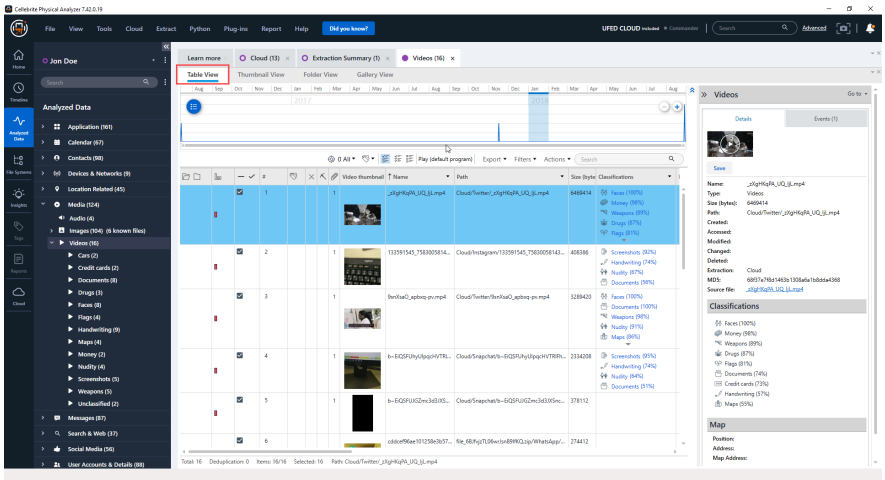
> If media classification was run on the extraction, you can double click the relevant category to open its tab. See Media classification (on page 346).



In the Videos tab, you can select the view you wish to see the videos. Available views include:

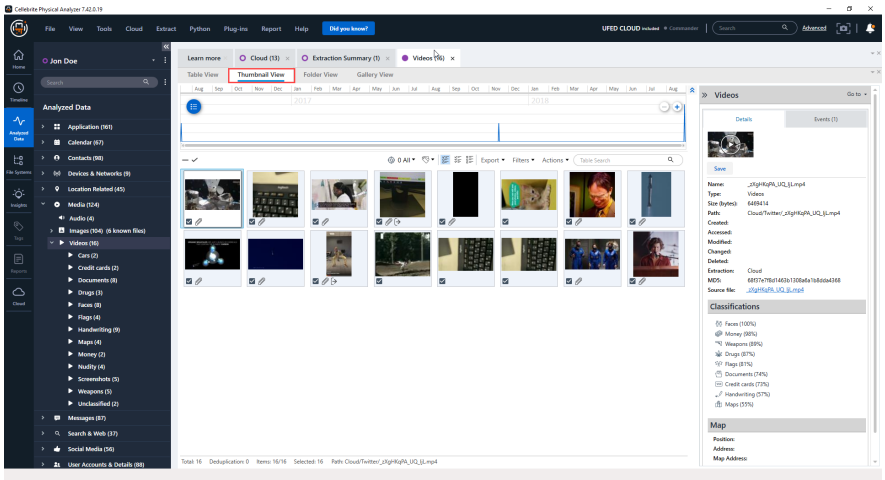
Table view

View a list of all videos in table format. Double click on a video to open in a separate tab.



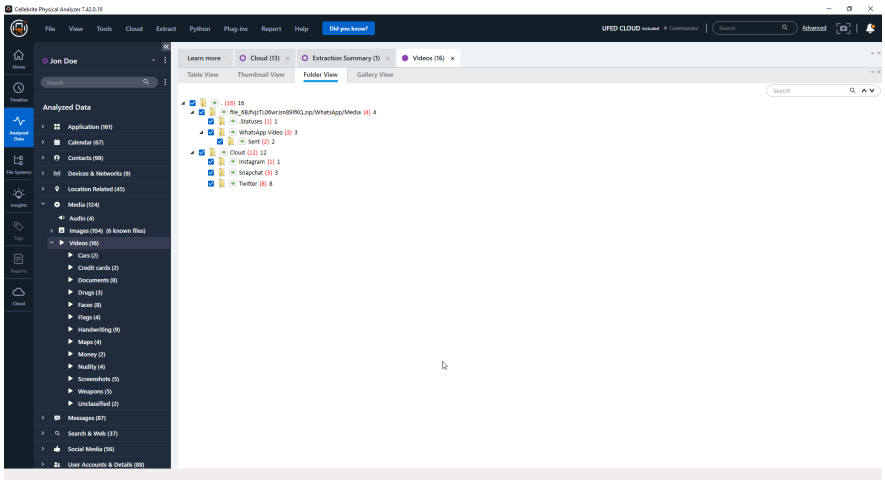
Thumbnail view

View videos by thumbnail. Double click the video to open in Gallery view.



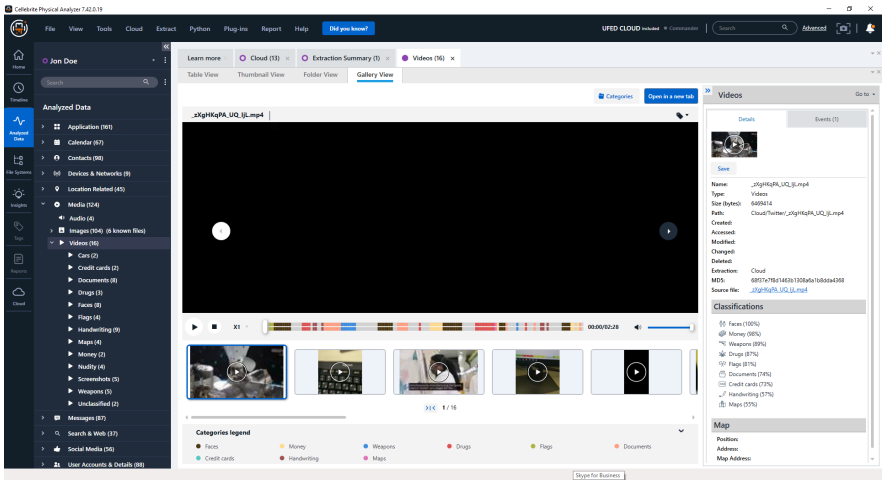
Folder view

View the folder structure of the data files paths in the reconstructed file system. Double click an item to open in Gallery view.



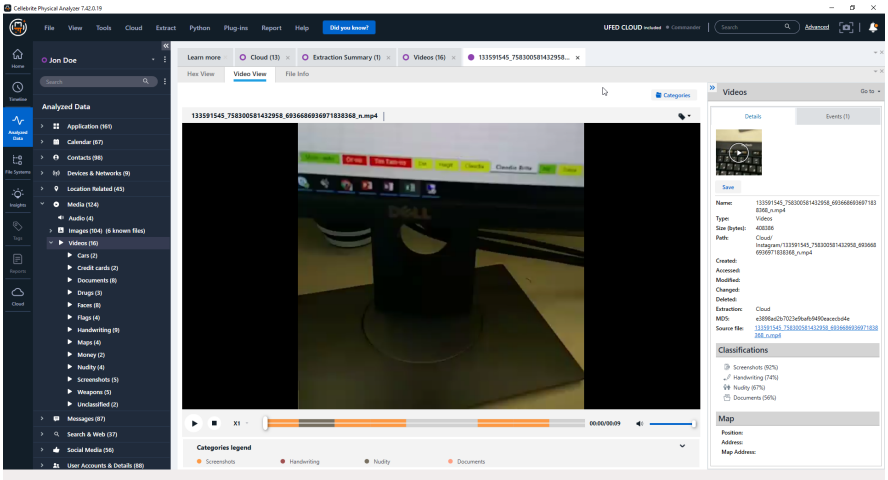
Gallery view

View videos in gallery format, easily scrolling through videos. If media classification was run on the extraction, view additional category details. See Viewing classified videos (on page 350).



Viewing single videos

1. In Gallery view, click **Open in a new tab** to view the video in a seperate tab.



The sub tabs for each video include:

- **Hex view** - view hex data for the video.
- **File info** - view the file information. For example, the File metadata section includes information such as the Capture Time, which is the date and time the video was taken.
- **Video view** - Play the video, view frames according to media categories.

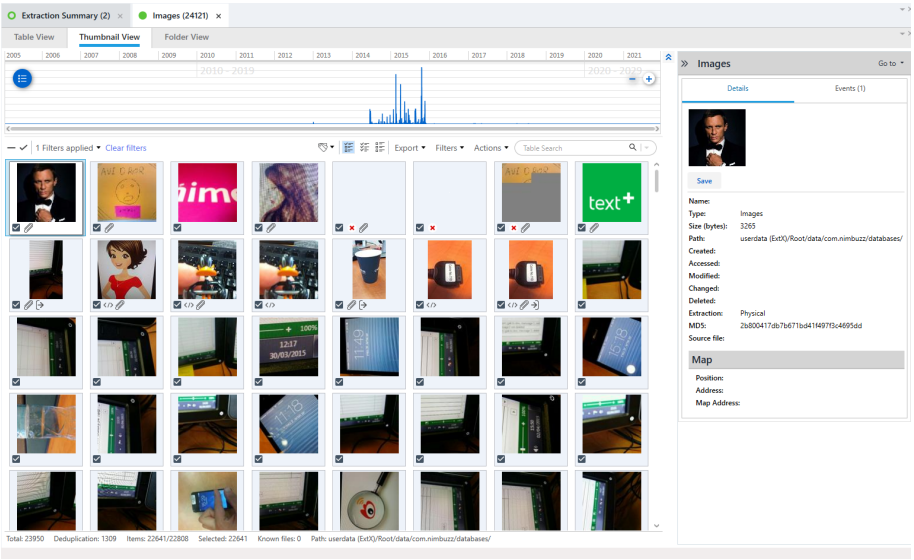
5.6. Redact content

Manually redact inappropriate images or videos. If a redaction has been performed, a redacted thumbnail will appear, and when generating reports, those marked files will be marked as redacted. You can also redact all attachments from your report in a single action when generating reports (for sensitive data or reduce size purposes).

The following procedures show how to redact and restore images. You can also perform these actions from the Videos tab.

To redact an image:

1. Go to Analyzed data > Media > Images.
2. Double click to open the Images tab. The following window appears.



3. Select the images.
4. Right-click the images and select **Redact**.

   or

   From the **Actions** menu select **Redact** (or use the hotkey Ctrl + F6). The following indicates that the image is redacted.

To restore a redacted image:

1. Select the images.
2. Right-click the images and select **Restore**.

   or

   From the **Actions** menu select **Restore**.

6. Locating and analyzing information

This section describes how to browse, search, filter, bookmark, and manage the information in your project.

6.1. Searching for information in a data tab

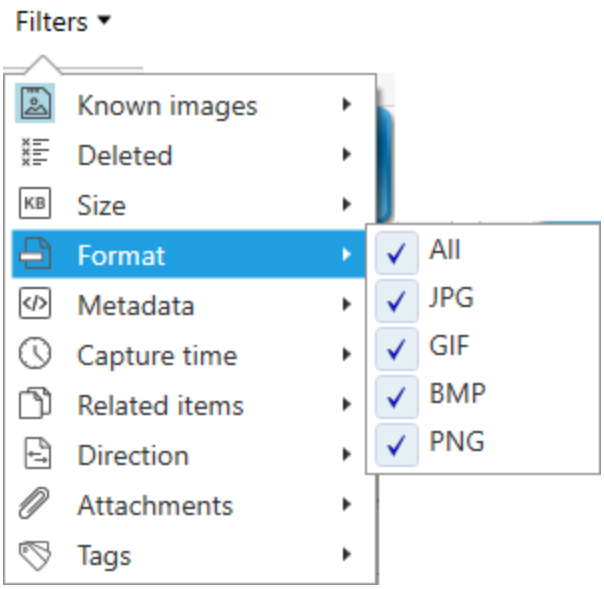
In **Table View** tabs, search for a particular item within the data table. The search is performed on all the data entries within the table.

» In the **Table Search** box, enter any string.

The table updates to display only items containing the string you entered.

6.2. Using the quick filter

To improve accessibility the filters are now grouped under simple menus. An example is displayed next.



Use the quick filters to filter data in Table View tabs.

	Only-non system	Display native or non-system images. Filter images that come with the device or as part of an app installation. By default, all system images are filtered. You can change this setting under **Settings** > **Data Files**.

	Show all	Display all items. This filter overrides the filters applied with the following three filters: Only selected, Only unselected, and Deleted.
	Only selected	Display only items that are selected.
	Only unselected	Display only items that are not selected.
	Deleted	Display only deleted items.
	Show all image sizes	Display all images. This filter overrides the filters applied with the following three filters: Display images above 30 KB, above 100 KB, and above 500 KB.
S	Display images above 30 KB	Display only small images above 30 KB.
M	Display images above 100 KB	Display only medium-sized images above 100 KB.
L	Display images above 500 KB	Display only large images above 500 KB.
	Filter images (by signature)	Click to enable file type filtering: JPEG, GIF, BMP, or PNG.
J	Show JPEG	Display JPG or JPEG files.
G	Show GIF	Display GIF files.
B	Show BMP	Display BMP files.
P	Show PNG	Display PNG files.
	Metadata	Filter image and video files by **Metadata** (**All**, **Without metadata** or **Has metadata**) and **Location** (**All**, **Has location** or **Without location**).

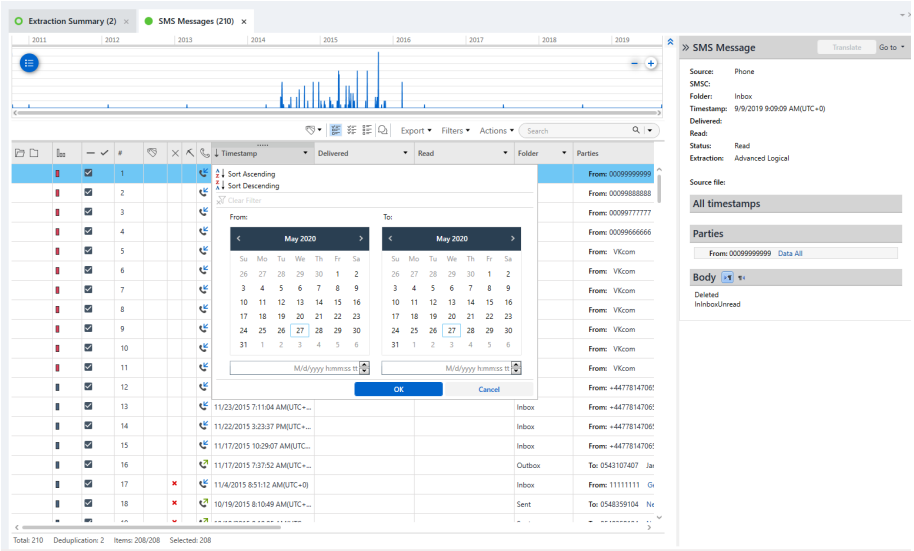
	Capture time	Filter image and video files by capture time. The maximum range is displayed by default, and you can select a specific date and time range.
	Translation filter	Filter translated text to display all text, translated text or text that has not been translated.
	Related items	Filter related items for extractions, which is very useful when working with the Multiple Extractions feature (see Analyzing multiple extractions (on page 70)). **All** displays all items, **Only deduplications** displays only items that include deduplications (duplicate or redundant data), **Only non-deduplications** displays only items that do not include deduplications, and **Only items with additional data** displays only items that include additional information.
	Translation commands	Translate all or selected texts, or delete translations.
	Conversation view	Open a conversation tab that displays the item and related messages.
	Open messages	Open all messages within a conversation in a table view.
	Attachment	Filter data files with attachments. **All** is for all data files, **Attachments** is for data files with attachments, and **Not attachments** is for data files that are not attachments.
	Attachment filter	Filter attachments that were sent or received. **All** is for all attachments, **Sent** is for attachments that were sent, **Received** is for attachments that were received, and **Unknown** is for unknown attachments.
	Attachment source app	Filter by the attachment's source app. All apps in the extraction are listed. Select the apps to display and then click **Finish**.
	Tag	Tag selected items.
	Remove tag	Remove a tag from the selected items.

	Manage tags	Open the Manage tags window.
	Open SQLite wizard	Open the SQLite wizard to build SQL queries and map database fields to Physical Analyzer models. For more information, see SQLite wizard (on page 307).
	Hide/view lower pane	Hide the lower pane with map item details. Click again to open the pane.
	Hide/view right pane	Hide the right pane with item details. Click again to open the pane.
Export	Export	Export the current view to an Excel (only hash values), Excel, HTML, PDF, XML, Word file, Project VIC (JSON), or GriffEye format (* C4P Index.xml). You can import the exported image or video files into Griffeye using a C4All XML data source.
	Location filter	Filter the locations displayed on the map.
	Retrieve address	Retrieve a physical address for the selected location.
	Group by	Group selected images or videos by time captured/recorded, created, modified, accessed, or deleted, or by camera make or model.
	Remove all filters	Remove all applied filters.

The toolbar items are context-sensitive, and only appear when relevant data is displayed.

6.3. Using the advanced filters

In any Analyzed data or Data file window, the listed results are filtered by column. Click on the relevant column heading to view filter and sort options. An example is displayed next.



When a filter is selected, only relevant results will be displayed.

6.4. Using advanced search

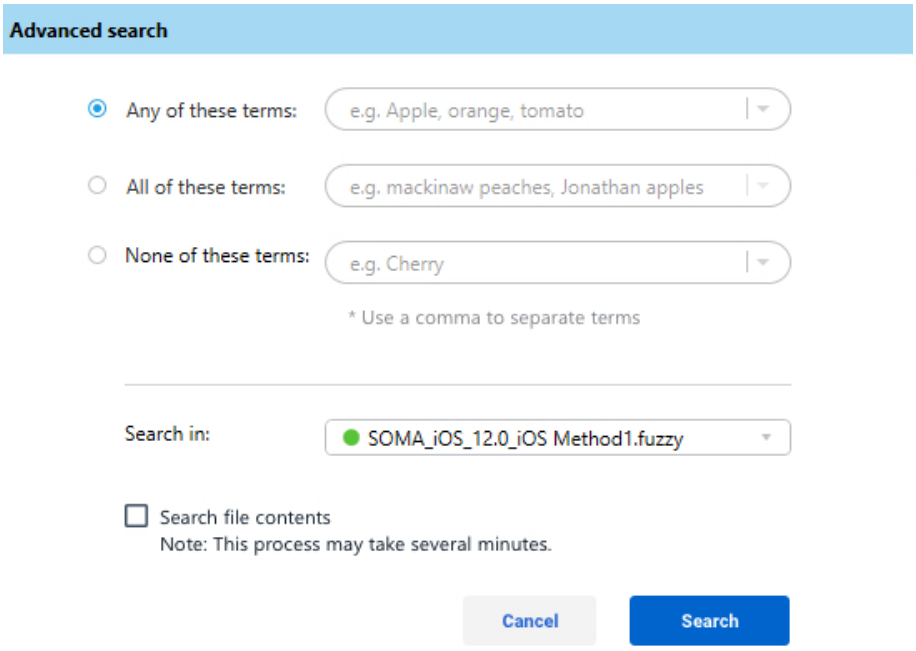
Using the new Advanced Search capability, narrow the scope of queries by applying filters and specifying additional requirements for a search. This functionality enables:

- Multiple keywords search
- And, or and exclude
- Searching in files content

To start using the Advanced Search:

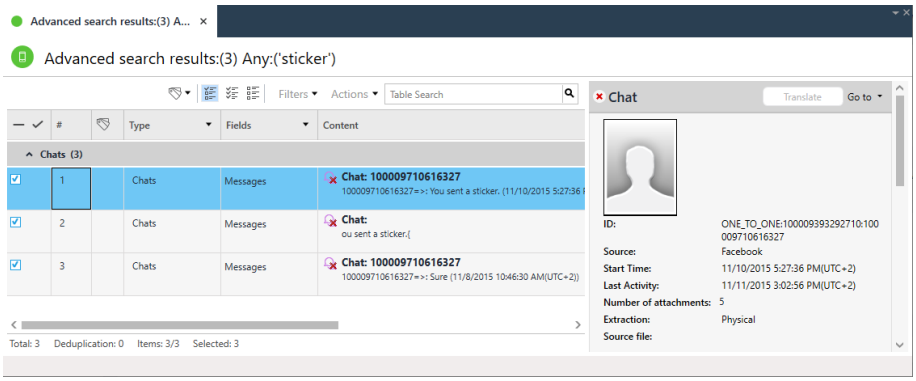
1. Click **Advanced** at the top right of the screen.

The following window appears.



2. Enter any, all or none of these terms.
3. Use a comma to separate terms.
4. Select the project (or search all projects).
5. Optionally select **Search file contents** to search in the contents of files within the extracted device (including file formats such as XML, plist, txt, DB, PDF, xlsx, DOCX, etc).
6. Click **Search**.

   Search results are presented in a separate Advanced search results tab, where you can view results, tag and mark items to include in your report.

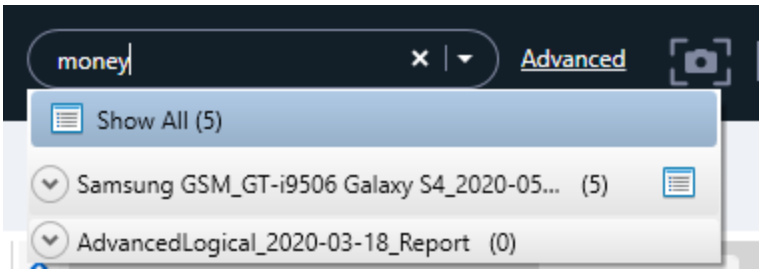


6.5. Searching for information in all open projects

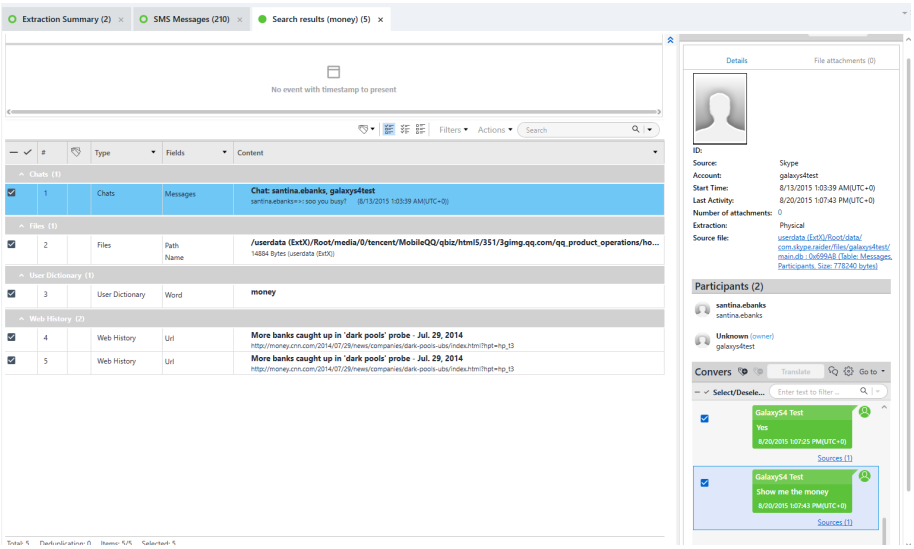
Use the all project search box in the toolbar to search for information in all open projects.

1. Type any string in the search box.

A list of matching results appear under the search box. The results are sorted by open project. Within each open project, the results are sorted by categories according to type (messages, contacts, files, and so on). The number of matching results found in each type category is also displayed.



2. Click to collapse or expand the projects.
3. Do one of the following:
   - Click next to the project name to view the results of the search in that extraction in a tab in the data display area.
   - Select **Show All** from the top of the quick results list to display a Search results tab in the data display area listing all the matching search results. The matching string in each item is indicated. As in the quick results list, the Search results tab lists the results by type. An example is displayed next.



You can create tags for the global search results items by selecting the **Tag All** or **Tag** options by clicking , however Device Info and folder files cannot be tagged.

Your recent search activity (up to 20 searches), including All projects search and table search are saved, until you close the application.

6.6. Browsing the file system

Physical Analyzer has the ability to reconstruct and display the device file system in a tree structure.

To browse the device file system:

1. In the **File Systems** view, click the ◢ or ▷ icons at every node to expand the tree item.
2. Continue drilling down in the file system to explore its content.

   Files in the reconstructed file system display one of the following icons:

   - - Existing file found in the system
   - - Deleted file data found in the file system
3. When you reach a file that you want to open, double-click it to display its information in the data display area.

   The number information tabs displayed for the file changes according to the file type. For example, an unknown file may display only the **Hex View** and **File info** tabs, while a jpeg image may display additional **Image view** and **Meta data** tabs. The default view is **Hex view**.

   For more information on working with Hex view, see Hex view (on page 116) and Working with hex data (on page 375)
4. While the Hex extraction of an image is displayed in the data display area, click a file under the **File Systems** tree to highlight the data portion of this file in the Hex data in the data display area.

6.7. Accessing conversation view

Communication-based data, such as call logs, email, Instant messages, and so on, can be displayed in a conversation view layout for easier and better tracking over the communication between two or more parties. You can search for messages within a chat, select the messages to include within a report (by default all chat messages are included), or export the conversation.

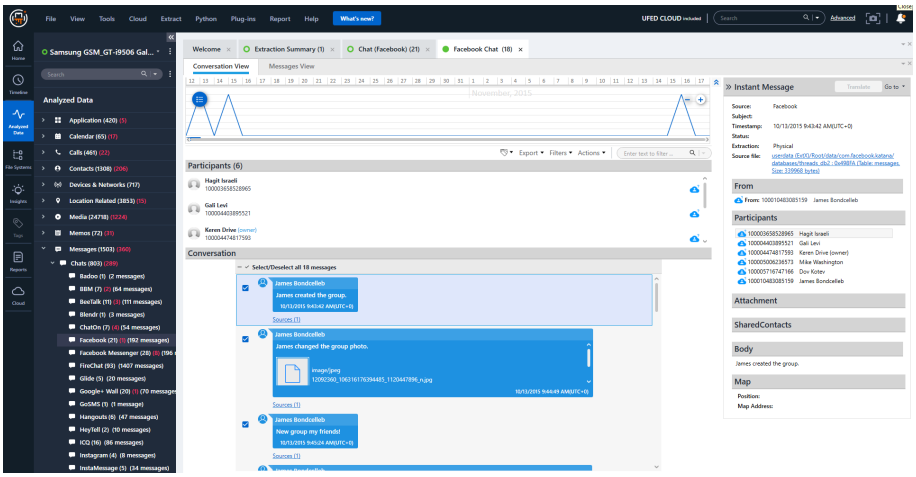
Messages in the conversation have an indication of how they were sent - PC, mobile, or Siri (for native iMessages).

In some cases, mainly when messages have been deleted, they cannot be forensically placed in a Chat. To maintain forensic accuracy of the messages, they will be placed in Instant messages and available for review under **Analyzed data > Instant messages**.

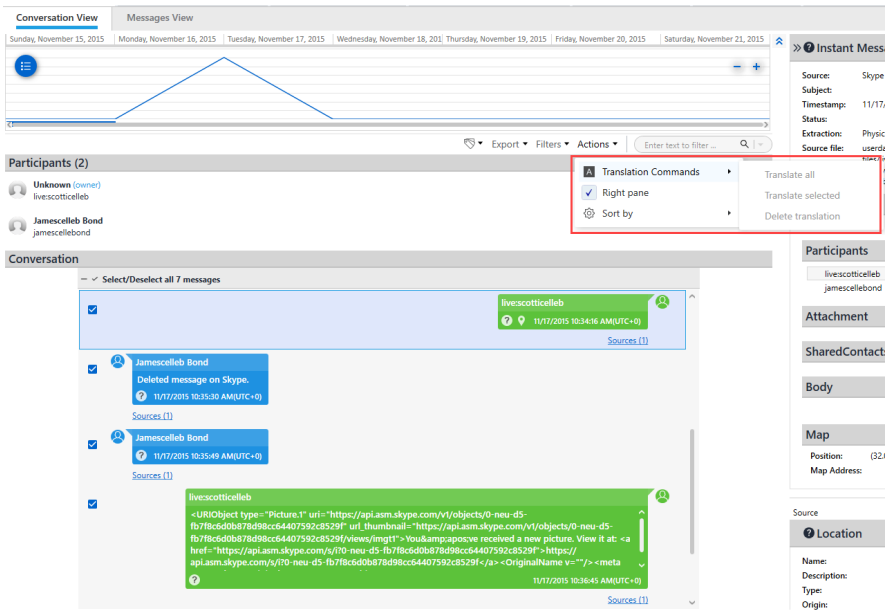
To access and use conversation view:

1. In a communication-based data table, select one of the records.
2. Click .

   A conversation tab opens, displaying related items as a conversation between the sending and receiving parties of the selected item.



3. To translate or delete translated text, click **Actions** and then select **Translate all**, **Translate selected** or **Delete all translations**.



4. To export the conversation, click **Export**.
5. Select the desired output:
   Excel, HTML, PDF, XML, or Word.
6. To change the order of the conversation, click **Actions > Sort by** and then select **Oldest message first**, or **Newest message first**.
7. To filter messages, enter text in the search box or click **Filter**.
8. To add or edit tags, click .
9. Select a check box to include specific messages in the report, (or select all messages or no messages).

6.8. Working with watch lists

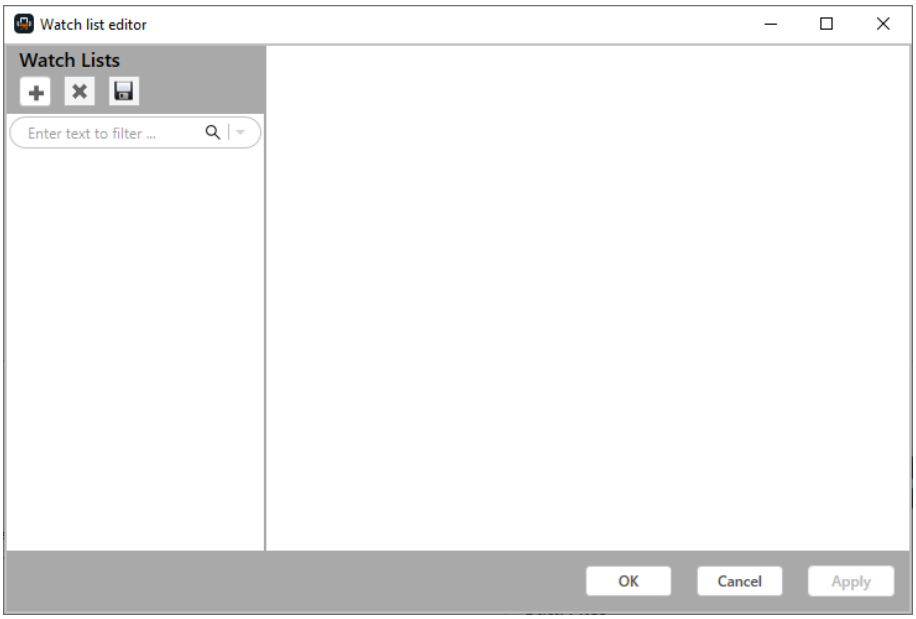
Run a watch list of keywords against your decoded data to identify and highlight the important and relevant information. Watch lists can either be activated automatically or run manually on selected decoded data.

Watch lists include the following:

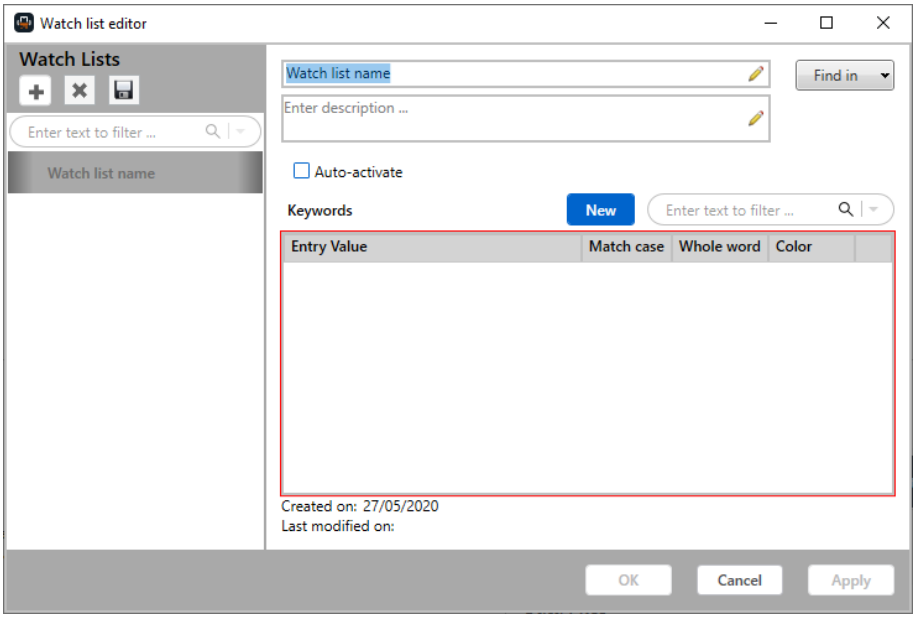
- Run multiple watch lists on the selected project.
- Receive notifications in the progress bar.
- View watch list results in a separate Watch List results window.
- Select, tag and incorporate watch lists results into your reports.

6.8.1. Creating a watch list

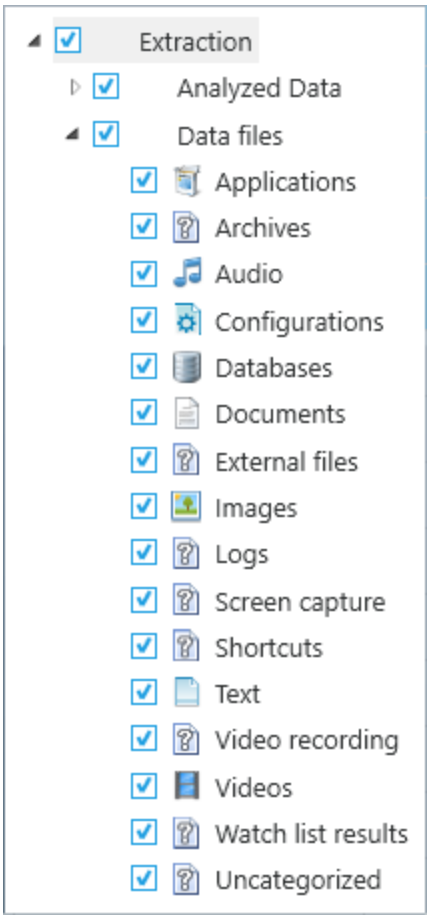
1. In the **Tools** menu, **Watch list > Watch list editor**. The Watch List Editor appears.



2. Click , and select **New**. The following window appears.



3. In the **Watch list name** box, enter a name for the watch list.
4. To set the watch list to find keywords only in Analyzed Data types or data files in the project, click **Find in**, and select the desired types.



When you run the watch list, only selected types are checked for matches.

5. In the **Enter description** box, enter a general description for the watch list (optional).
6. To set the watch list to run automatically when you open projects, click **Auto-activate**.
7. Click **New** to add a new keyword. A new keyword row appears in the Keywords list.
8. For each keyword, set the following, as desired:
   - **Entry Value**: Enter the keyword.
   - **Match case:** Select to match the case of the keyword
   - **Whole word:** Select to match the whole keyword.
   - **Color:** Click ▾ and select the color you want matched keywords to be shown in.
9. Do one of the following:
   - Click **Apply** to save the watch list and keep the Watch List Editor open.
   - Click **OK** to save the watch list and close the Watch List Editor.
   - Click **Cancel** to close the Watch List Editor without saving your changes.

6.8.2. Editing a watch list

1. In the Watch List Editor, select the watch list that you want to edit.
2. Edit the watch list parameters and keywords that you want to change.
3. To filter the keyword list to locate a particular keyword, type the keyword in the **Enter text to filter** box.
4. To edit a keyword, click the relevant keyword in the list, and make the desired changes.
5. To delete a keyword, click ✕.
6. When you have finished making changes, do one of the following:
   - Click **Apply** to save the watch list and keep the Watch List Editor open.
   - Click **OK** to save the watch list and close the Watch List Editor.
   - Click **Cancel** to close the Watch List Editor without saving your changes.

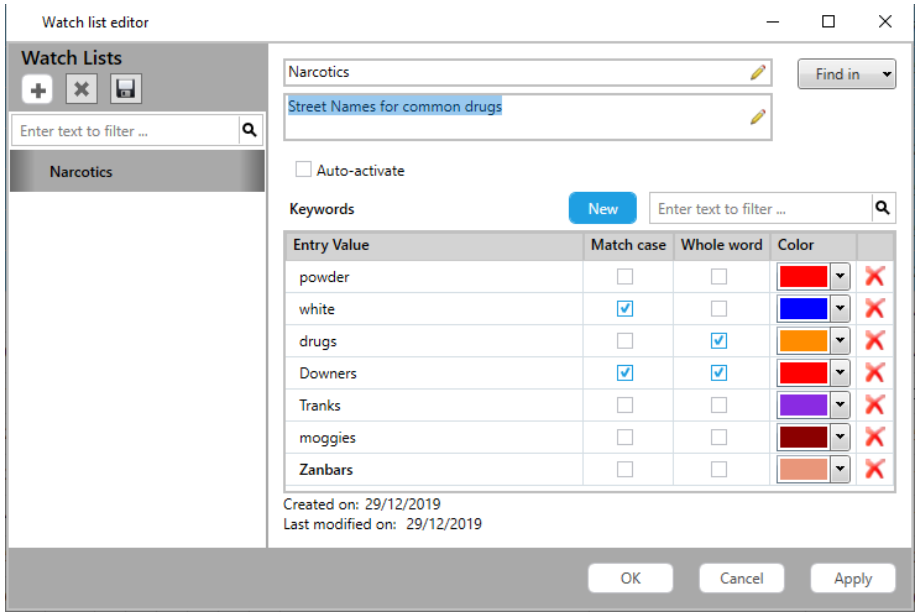
6.8.3. Importing a watch list

The export and import functions enable you to share watch lists and receive watch lists from your colleagues. Import existing watch lists (*.csv files) that were saved from or created by Physical Analyzer.

You can also import a CSV file with each keyword on a separate line. This option will import the keywords without any formatting and will set all data types by default.

1. In the **Tools** menu, select **Watch list editor**. The Watch List Editor appears.
2. Click ✚, and select **Import**.
3. Browse to the location where your watch list is saved, select the CSV file, and click **Open**.

   The watch list appears in the Watch List Editor. An example is displayed next.



6.8.4. Exporting a watch list

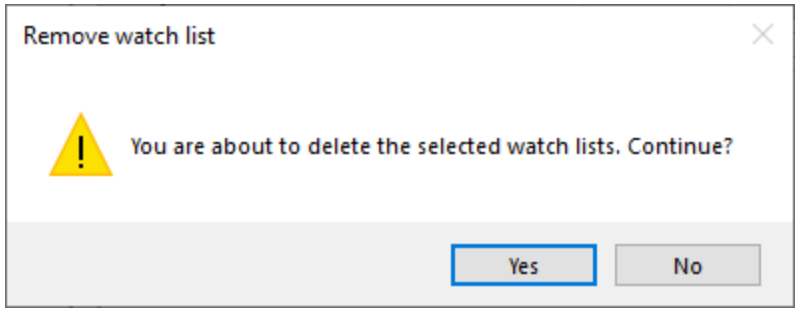
Export watch lists to save the watch list as a *.csv file for later use, or to share with others.

1. In the Watch List Editor, select the watch list that you want to export.
2. Click .
3. Browse to the location where you want to save your watch list, and click **Select Folder**.

   The watch list is exported. It will be saved by default as [name of watch list].csv.

6.8.5. Deleting a watch list

1. In the Watch List Editor, select the watch list that you want to delete.
2. Click . The following window appears.

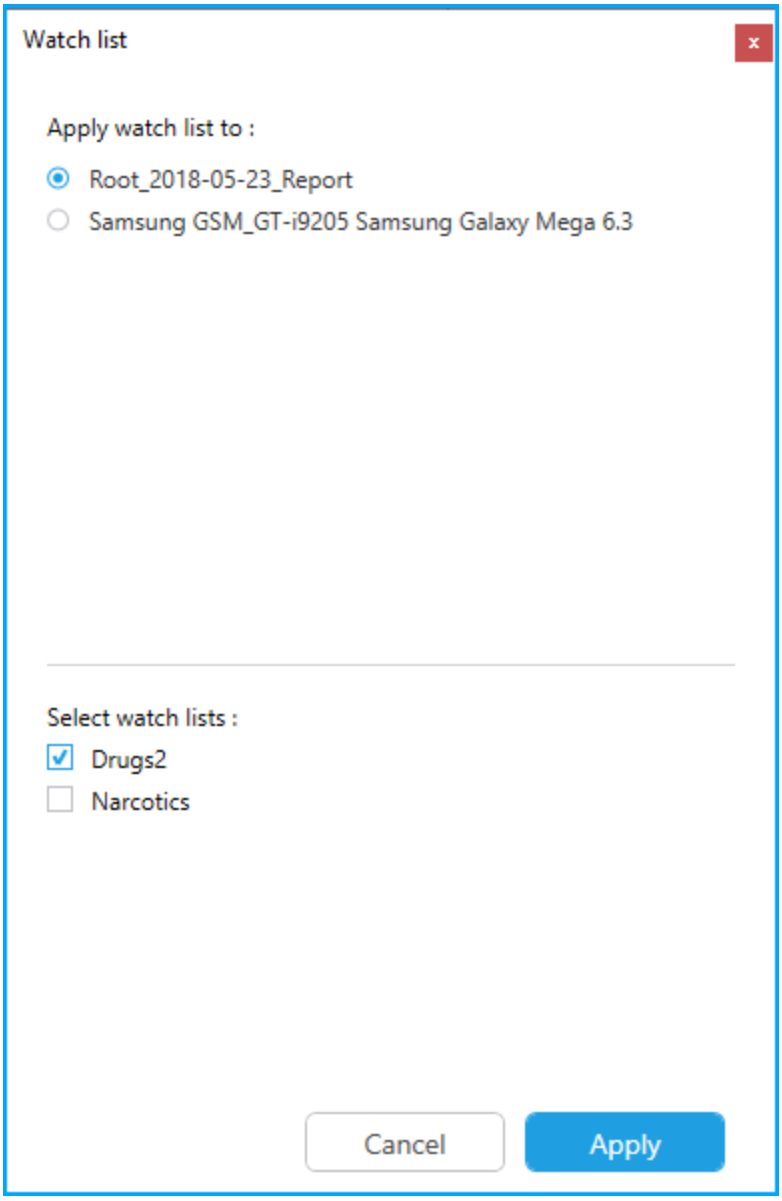


3. Click **Yes**. The watch list is deleted.

6.8.6. Running a watch list

When you run a watch list from the Watch List Editor, you can select which watch lists to run, and on which projects you want to run them.

1. Select **Tools** > **Watch list** > **Run watch list**. The following window appears.

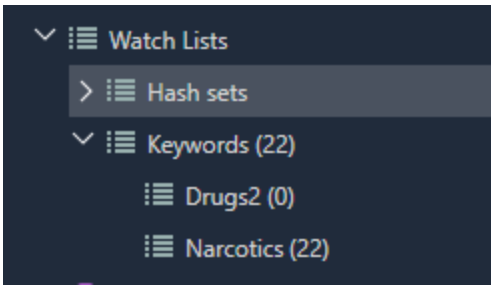


2. Select the open project that you want to run the search on and the required watch lists.

> A tick mark ✓ shows that the selected watch list is currently active for the project.

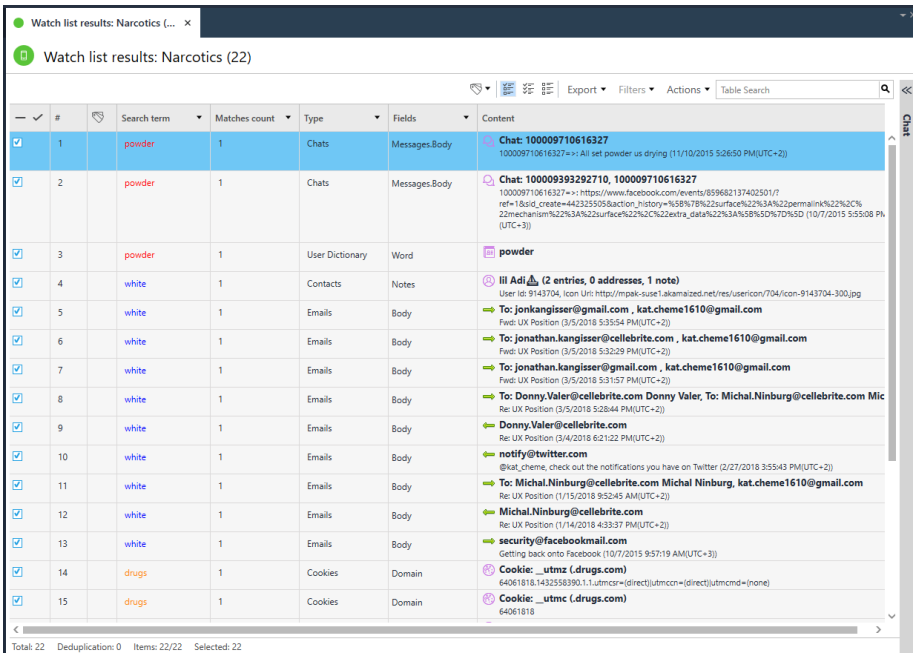
3. Click **Apply**.

Physical Analyzer searches for keywords in the selected project. When complete, the watch list results appear in the **Watch Lists** tree item in the Insights view.

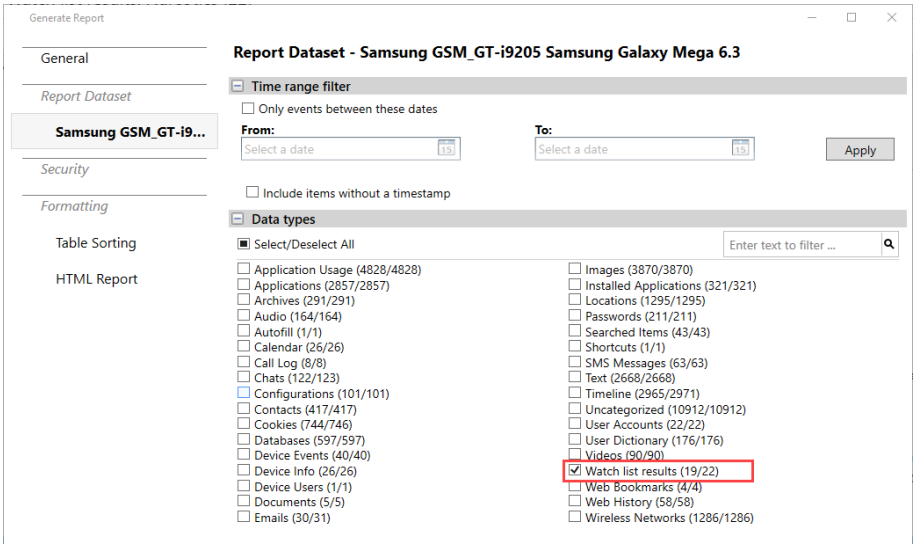


If the watch list is assigned to only particular information types (see Creating a watch list (on page 145)), only matches to those types appear in the watch list results.

4. Double-click the watch list results from the tree item to open the Watch list results window.



From this window you select, tag and incorporate watch lists results into your reports. An example from the report wizard displayed next.



6.8.7. Locating a watch list

1. In the **Tools** menu, select **Watch list > Watch list editor**. The Watch List Editor appears.
2. In the **Enter text to filter** box, enter the watch list name in whole or in part and click 🔍. The list of watch lists is filtered accordingly.

6.9. Importing and categorizing hash sets

Hash database files are used to compare the MD5 hash sets of images, videos and files in an extraction to databases of known and blacklisted files. This feature provides the capability to quickly identify media related to child exploitation, and incriminate predators. Physical Analyzer enables you to create hash databases by importing Project VIC and CAID files, and matching them against media recovered as part of the extraction, specified with the appropriate Project VIC/CAID category. In addition, you can also upload any CSV or text file which contains a list of known hash values, and match it against any file recovered from the device.

The Hash set feature supports the following types of files:

- **Project VIC:** An ecosystem of information and data sharing between domestic and international law enforcement agencies all working on crimes facilitated against children and the sexual exploitation of children. Project VIC compiled all existing online child abuse images into a single repository. Each image, whether still or video, has a unique identifier known as a "hash value." Using the hash value allows investigators to quickly rule images in or out of their searches. For more information, refer to http://www.projectvic.org/
- **CAID:** The Child Abuse Image Database. CAID uses the latest technology to transform how we deal with images of Child Sexual Exploitation and Abuse. It brings together all the images that the Police and NCA encounter. Forces then use the images' unique identifiers – called hashes - and metadata to improve how they investigate these crimes and protect children. The Home Office developed CAID in collaboration with the police, industry partners and British and international Small and Medium Sized Enterprises (SMEs). CAID went live with seven police forces in December 2014. All UK territorial police forces and the National Crime Agency are now connected to CAID. For more information, refer to https://www.gov.uk/government/publications/child-abuse-image-database
- **Text and CSV:** Any text or CSV file with MD5 hash sets/values in one column with all hash set values, without headers.

For more information, see the following sections:

Managing hash sets (on the facing page)

Adding a hash set (on page 156)

Running hash sets (on page 158)

Editing, updating and deleting hash sets (on page 162)

Exporting the hash database (on page 163)

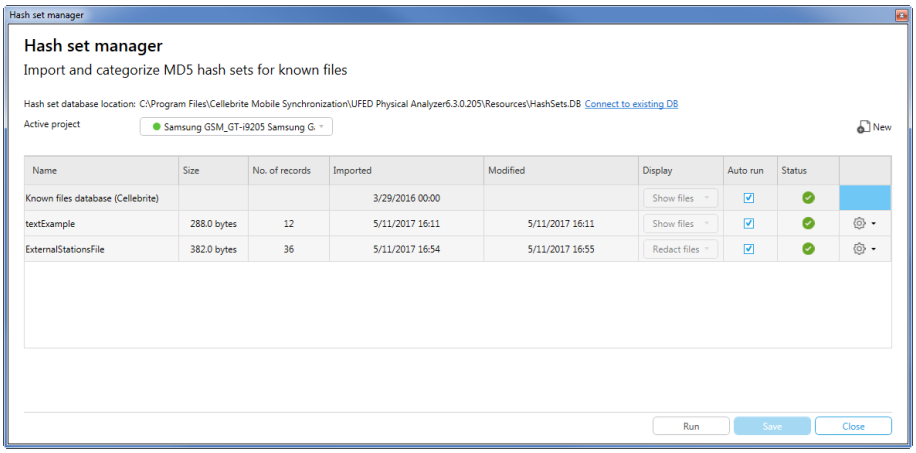
6.9.1. Managing hash sets

This section includes the following:

- Accessing the hash set manager
- Moving the hash set database location
- Connecting to a hash set database

To access the hash set manager:

- From the **Tools** menu select **Watch List** > **Hash set manager** (or Ctrl+H). The following window appears.



This Hash set manager window displays information and enables you to perform actions, as follows:

Option	Type	Description
Connect to existing DB	Link	Connect to a new or shared hash set database location.
Active project	List	Select the active Physical Analyzer project.
New	button	Create a new hash set. For more information, see Adding a hash set (on page 156).
Name	Field	Name of the hash set.
Size	Field	Size of the hash set.
No. of records	Field	Number of records in the hash set.
Imported	Field	Date the hash set was imported into Physical Analyzer.
Modified	Field	Date the hash set was last modified.

Option	Type	Description
Display	Field	Interface display settings for the hash set: Show files or Redact files.
Auto run	Field	Auto-run the hash set as part of the automatic decoding process.
Status	Field	Indication if the hash set is ready to be run.
	Menu	Edit update or delete hash sets.
Run	Button	Run the hash sets against the active project.
Save	Button	Saves any changes that you made to the Hash set manager.
Close	Button	Close the Hash set manager.

You cannot edit or delete the default hash set: `Known files database (Cellebrite)`. This hash set is used to categorize images that appear under the Data Files tree item.

Common/Known Image Filter: As part of the decoding process, Physical Analyzer can calculate hash values of any extracted data file, particularly for media files. Physical Analyzer automatically filters out common images. This saves time that would otherwise be spent reviewing common media images that are device files, device icons or images that are part of an app's installation.

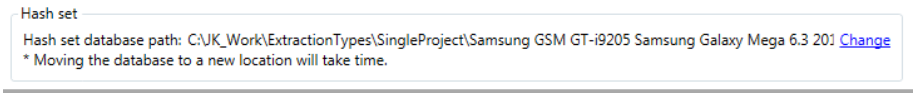
Moving the hash set database location

If required, you can move the hash set database to a new location. Other users can then use the connect procedure below to connect to this new location.

Depending on the size of the database, moving it to a new location will take time to complete.

To change the hash set database location:

1. Go to **Tools** > **Settings**. The General Settings window appears. For more information on settings, see General settings (on page 421).
2. In the Hash set area, click **Change**.



3. Select the required location.
4. Click **Select Folder**.
5. Click OK.

6.9.1.1. Connecting to a hash set database

After a database is moved to a new location, other users can use the connect procedure below to connect to this new or shared location.

To connect to a different hash set database:

1. Click the **Connect to existing DB** link.

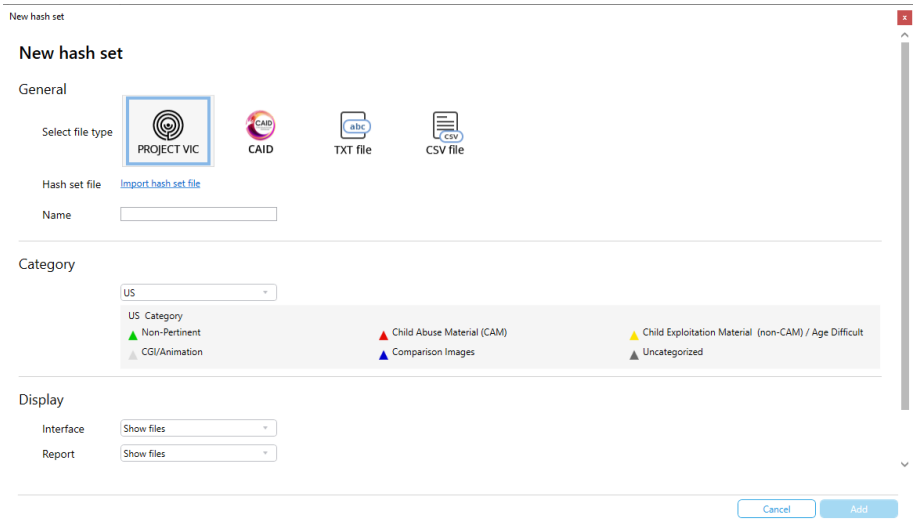
> The default location is:
> C:\Users\<username>\AppData\Roaming\Cellebrite Mobile Synchronization\HashSets\HashSets.DB

2. Browse to the location of the required hash set database.
3. Click **Open**.

6.9.2. Adding a hash set

To add a new hash set:

1. Click **New** (New). The following window appears.

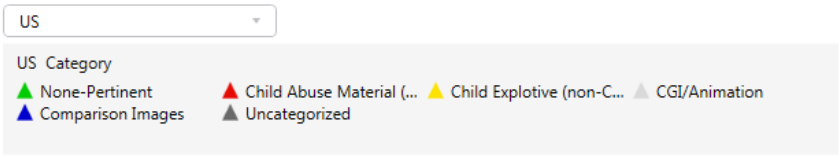


2. Select the file type: Project VIC, CAID, TXT file, or CSV file.

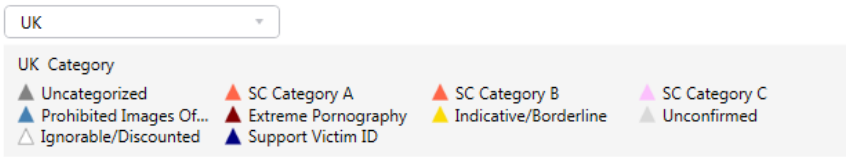
> After the hash set is added, the selected file type cannot be changed.

3. Click **Import hash set file**, select the required file and click **Open**.
4. Enter a name for the imported file or use the default name.
5. If you are importing a Project VIC file select a category, as displayed next. For each category, relevant category colors are displayed. CAID is automatically set to the UK category.

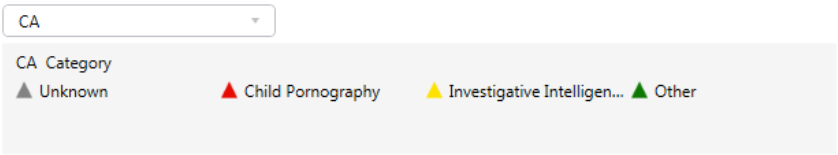
   - **US:** United States of America. This includes the following categories:



   - **UK:** United Kingdom. This includes the following categories:

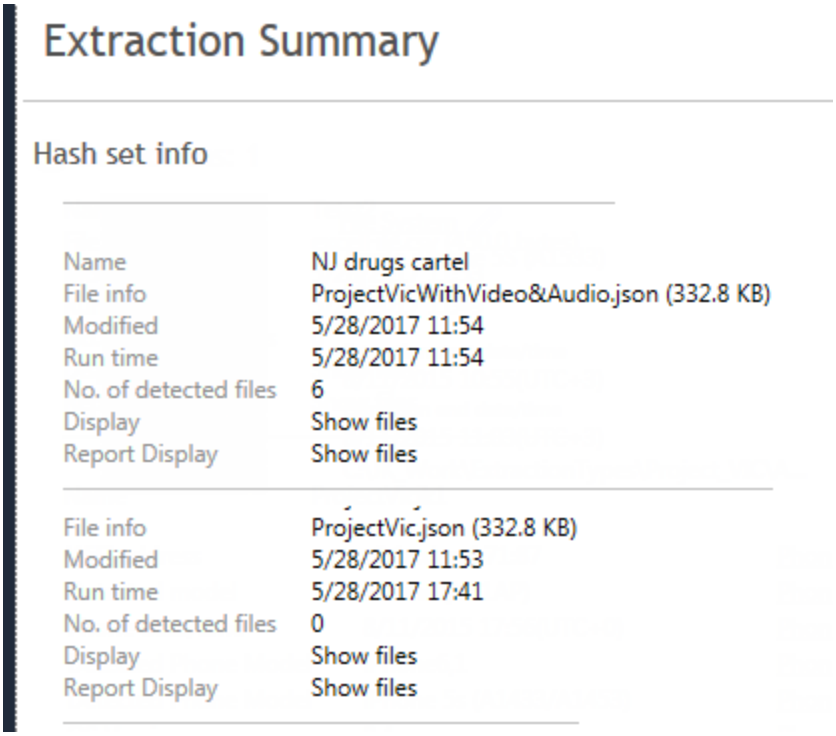


» **CA:** Canada. This includes the following categories:



6. In the Display area select how the results are displayed. You can show or redact files, for each of the following:
   » **Interface:** Select how the resulting files will be displayed in the Physical Analyzer user interface.
   » **Report:** Select how the resulting files will be displayed in the Physical Analyzer reports.
7. Click **Add**. A new row is added to the table. For information on running a hash set, see Running hash sets (on the next page).

> The Extraction Summary window displays information about each hash set including: name, file information, date modified, date run, number of detected files, display settings, and report settings. An example is displayed next.



Extraction Summary

Hash set info

Name	NJ drugs cartel
File info	ProjectVicWithVideo&Audio.json (332.8 KB)
Modified	5/28/2017 11:54
Run time	5/28/2017 11:54
No. of detected files	6
Display	Show files
Report Display	Show files

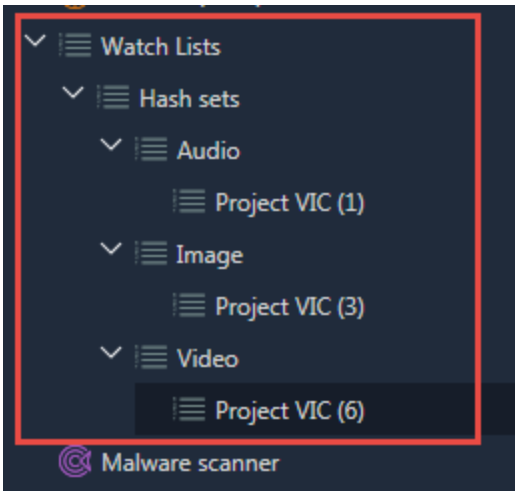
File info	ProjectVic.json (332.8 KB)
Modified	5/28/2017 11:53
Run time	5/28/2017 17:41
No. of detected files	0
Display	Show files
Report Display	Show files

6.9.3. Running hash sets

To run hash sets:

» In the Hash set manager window, click **Run**.

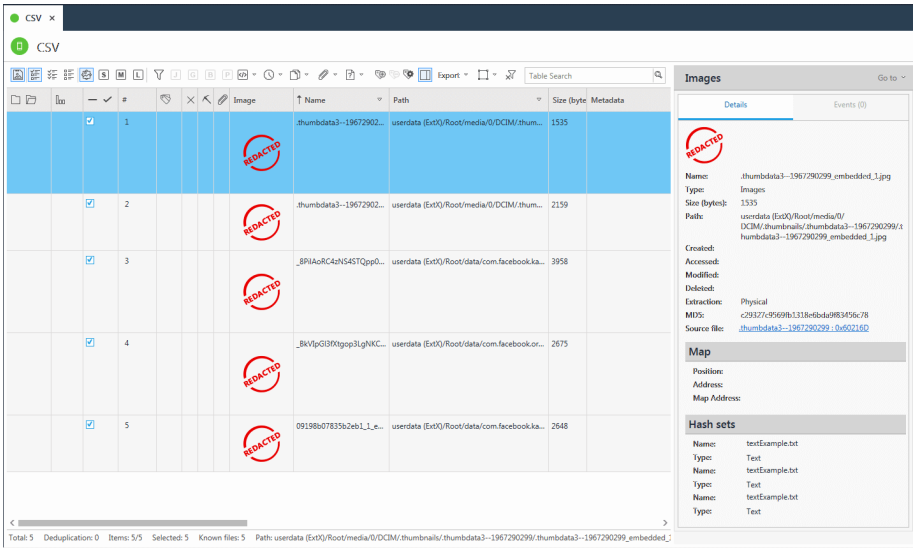
After you run the hash set the matching results are displayed in the project tree on the left under Watch list > Hash sets.



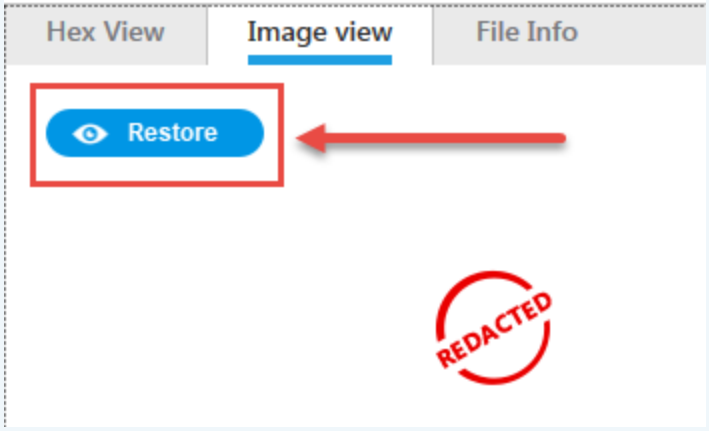
6.9.3.1. Examples

6.9.3.1.1. Redacted images

An example with redacted image results is displayed next.

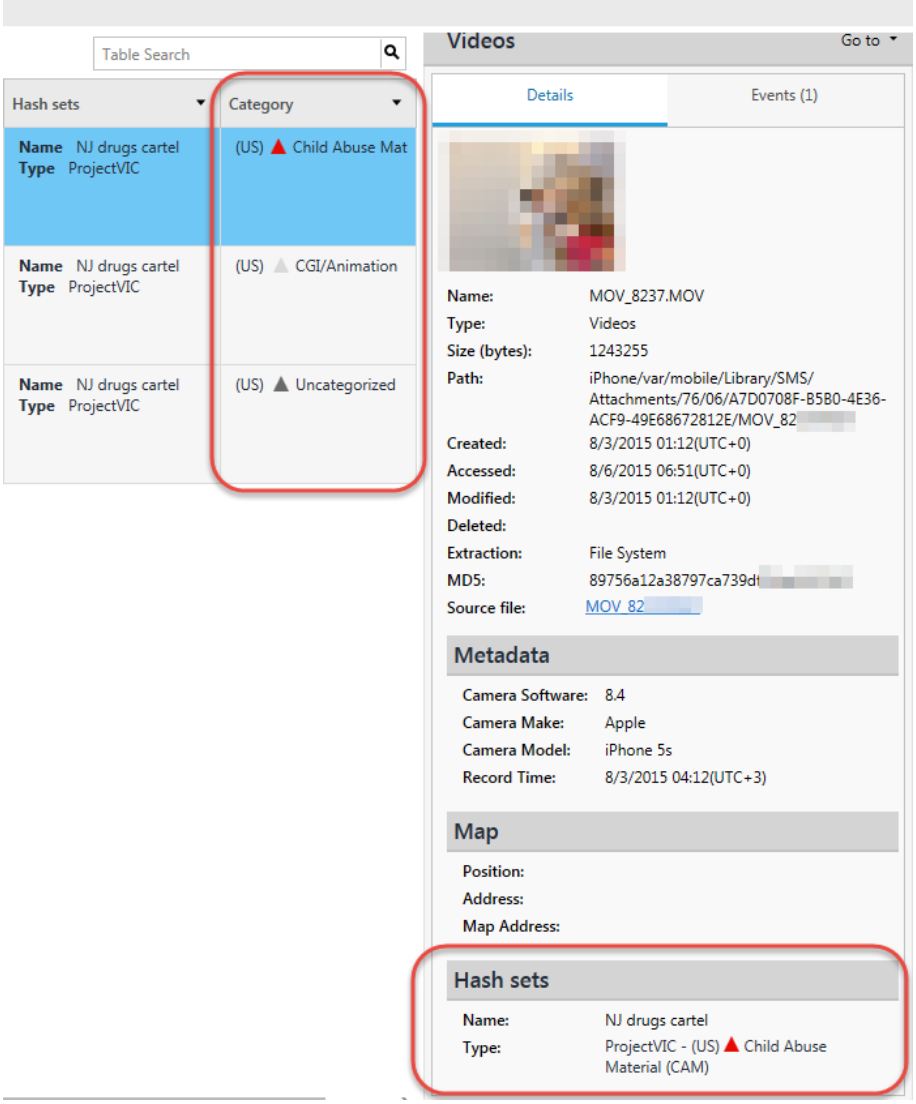


To view the redacted image, double-click the required image and in the Image view tab click **Restore**.



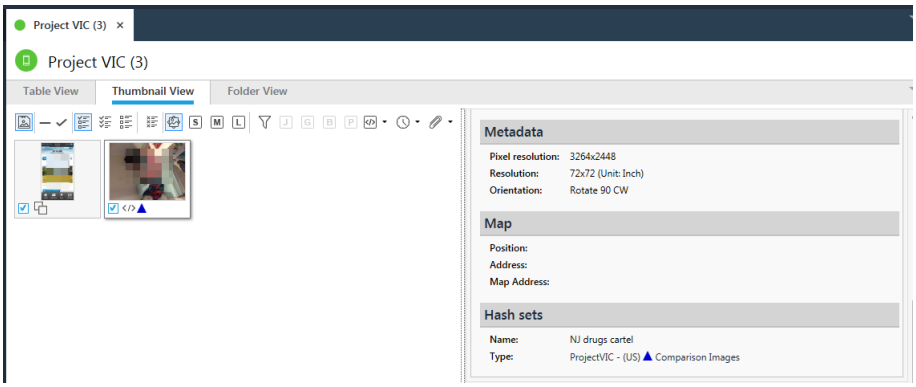
6.9.3.1.2. Project VIC categories

An example with matching Project VIC categories is displayed next.



6.9.3.1.3. Thumbnail view

A thumbnail view example, with a Project VIC category is displayed next.



TXT and CSV matches are indicated with a Yellow H as displayed next.

6.9.4. Editing, updating and deleting hash sets

> You cannot edit or delete hash sets while Physical Analyzer projects are open. Close all projects and try again.

To edit the hash set properties:

1. Close all open extractions.
2. Select the required hash set record in the table.
3. Click and select **Edit hash set properties**.
4. Edit the properties.
5. Click Save.

To update the records in a hash set file:

> This option is useful if you want to add an update to an existing hash set. For example, Project VIC sends regular update files.

1. Select the required hash set record in the table.
2. Click and select **update file**.
3. Select the file that you want to update.
4. Click **Open**.

> When using the Update file function, only additional unique records will appear under the Number of records column. Deleted records are not indicated.

To delete a hash set:

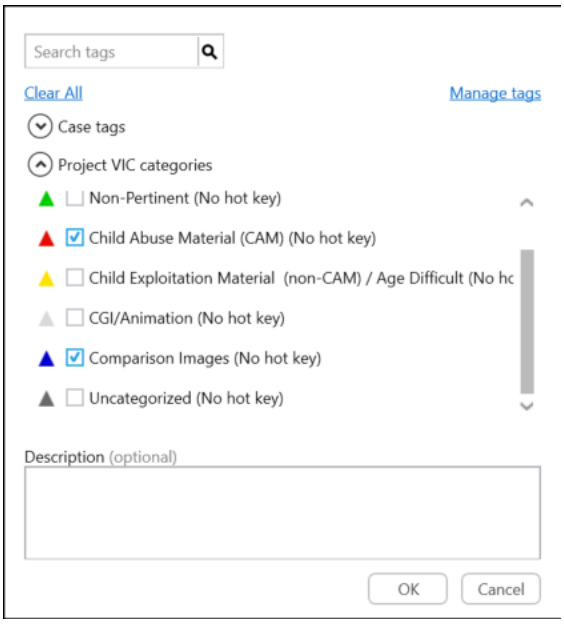
1. Close all open extractions.
2. Select the required hash set record in the table.
3. Click and select **Delete hash set**.
4. Click Yes.

6.9.5. Exporting the hash database

To participate in the fight against child sexual exploitation and trafficking export and share your manually tagged media files. The export creates a JSON file that includes a hash of offending photos, which you can share with Project VIC and CAID. The hash can contain all the original metadata of the image.

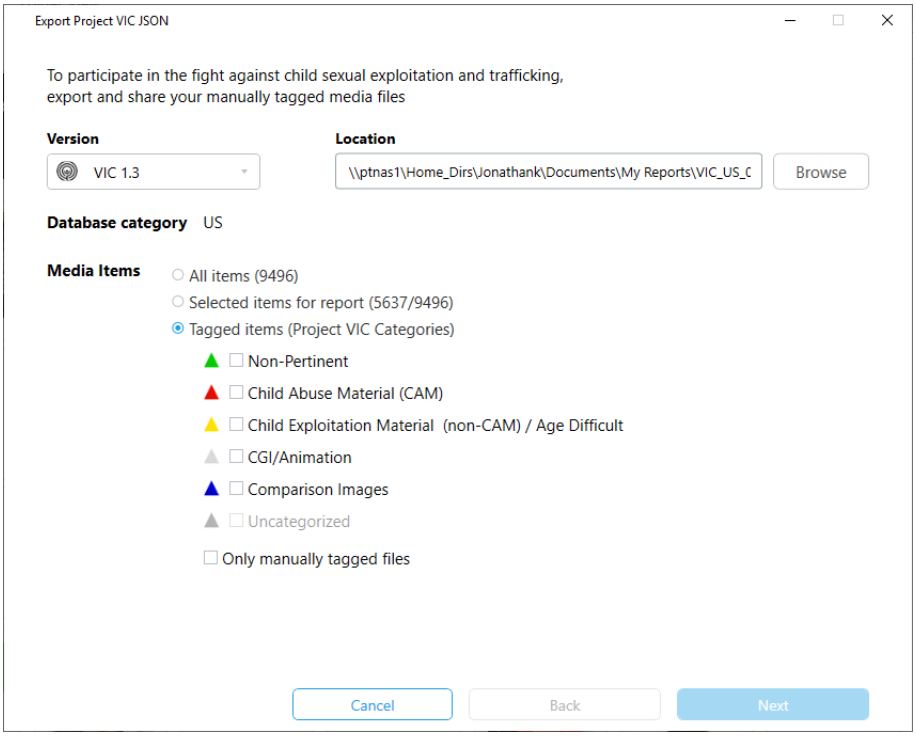
To export the hash database:

1. Click to tag your media files. The following window appears.

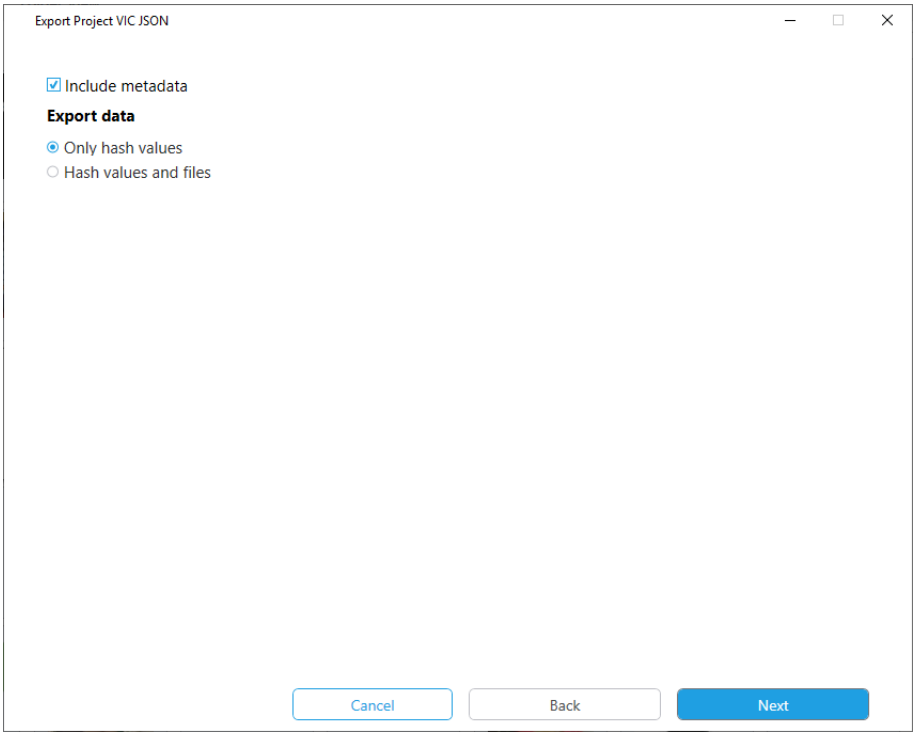


> You can change the Project VIC/CAID categories under **General settings** > **Hash set**. For more information, see General settings (on page 421).

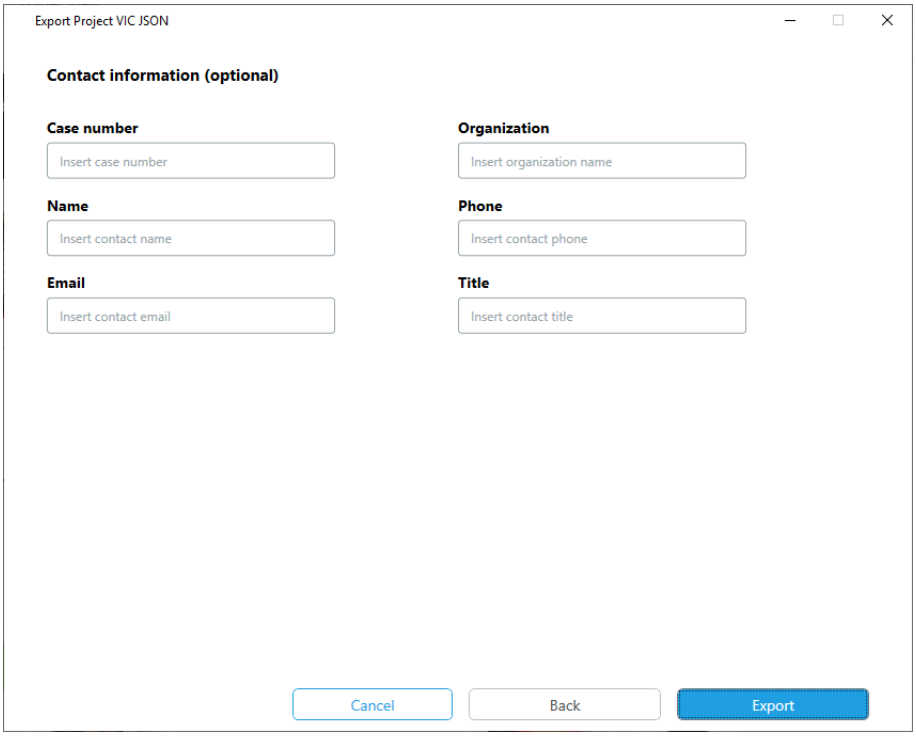
2. Tag your media files using Project VIC/CAID categories.
3. Select **Tools** > **Watch list** > **Export Hash database**. The following window appears.



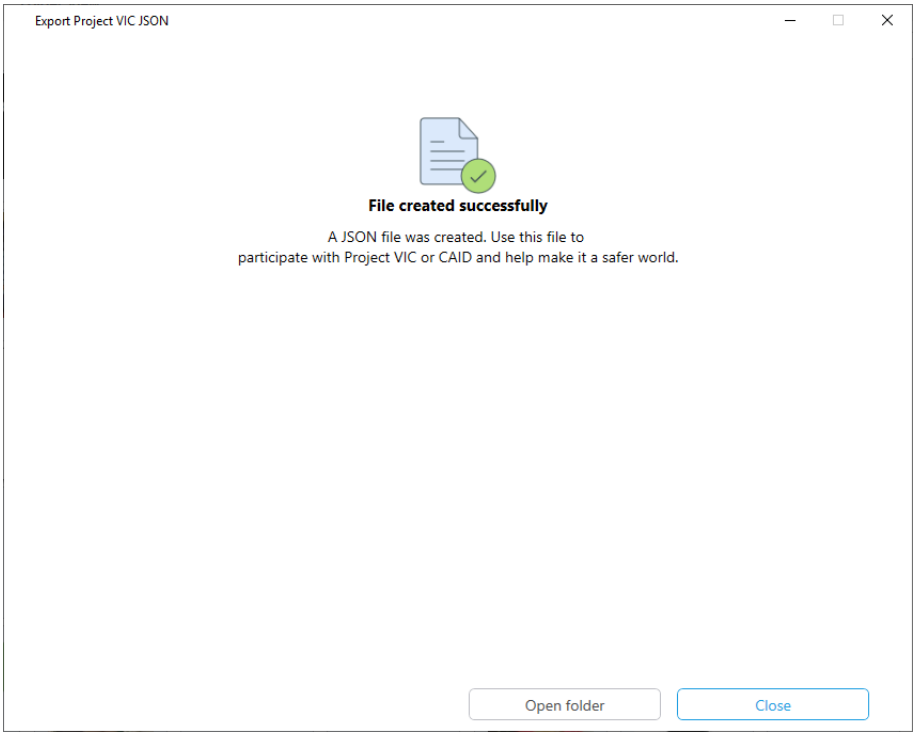
4. Select the project VIC version (i.e., VIC 1.3 or VIC 2.0).
5. Select the current location of the export file or click **Browse** to choose another location.
6. Select the media items to export as follows:
   - **All items:** Includes all media files.
   - **Selected items for report:** Includes all media files that we marked to be included in the report.
   - **Tagged items (Project VIC categories):** Includes all media files with Project VIC/CAID categories. You can also select the check boxes for only the required categories.
   - **Only manually tagged:** Includes the media files that you manually tagged with Project VIC/CAID categories.
7. Click **Next**. The following window appears.



8. Select to include all the original metadata of the media.
9. Select the data to export. Only the hash values or the hash values and the files.
10. Click **Next**. The following window appears.

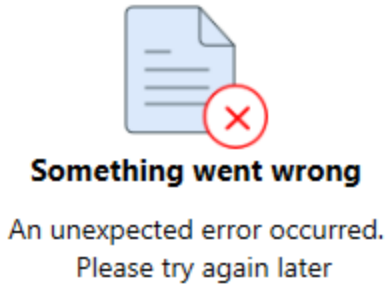


11. (Optional) Enter the case information.
12. Click **Export**. The following window appears.



13. Click **Open folder** to locate the JSON file and then share the file with Project VIC or CAID.

    If no files are selected to be exported an error message will be displayed.



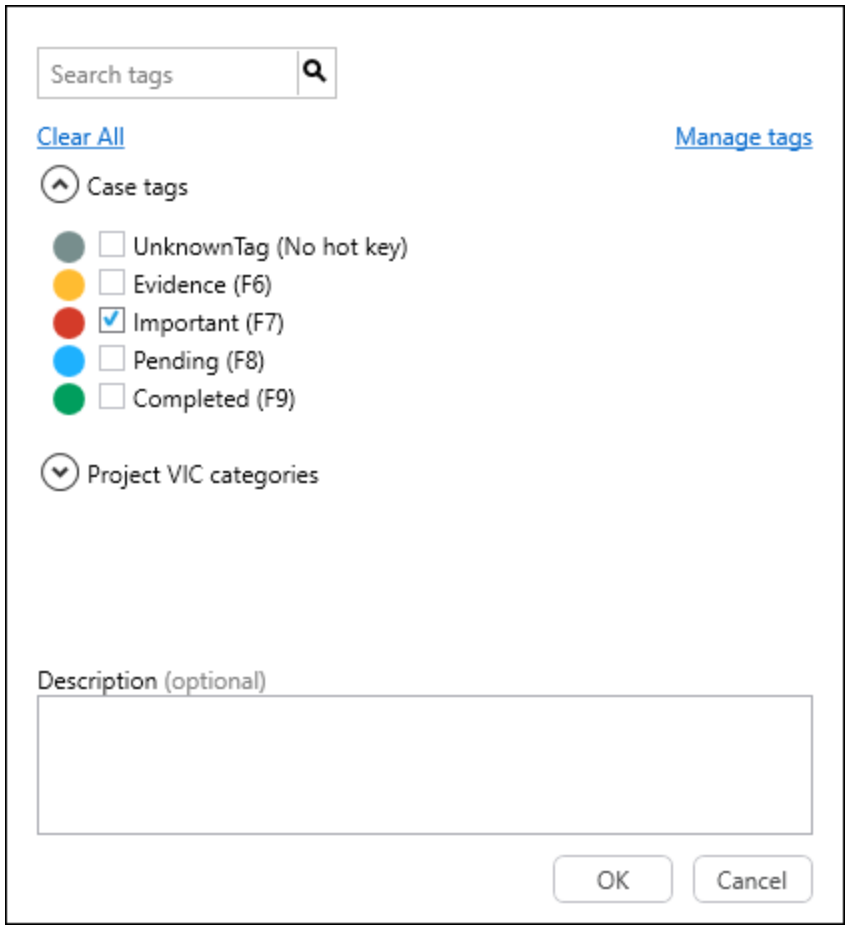
6.10. Tags

While reviewing events, contacts, etc., the investigator can tag items for future reference. Each item can have multiple tags. A tag is essentially a quick reference you can create on individual items:

- An **Analyzed Data** item such as a call from the call log, a contact record, an email message, etc. See Analyzed data (on page 89).
- A **Data Files** item such applications, archives, configurations, databases, and so on. See Data files (on page 90).

To tag an item:

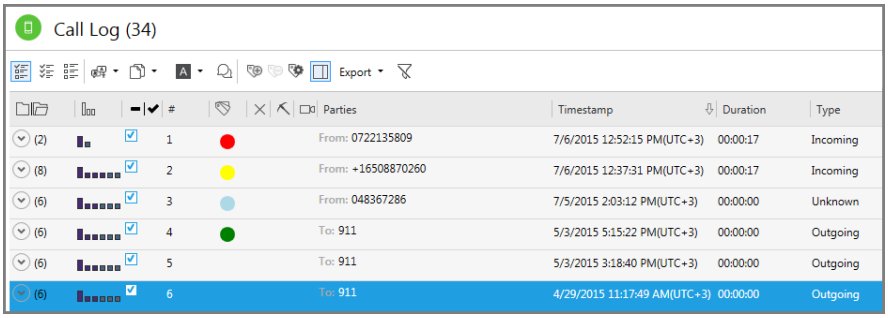
1. Click . The following window appears.



> The window also includes Project VIC or CAID categories. For more information, see Importing and categorizing hash sets (on page 152).

To display other Project VIC/CAID categories, go to **General settings** > **Hash sets**.

2. Choose the relevant tag and click OK. An example is shown next. For more information, see General settings (on page 421).



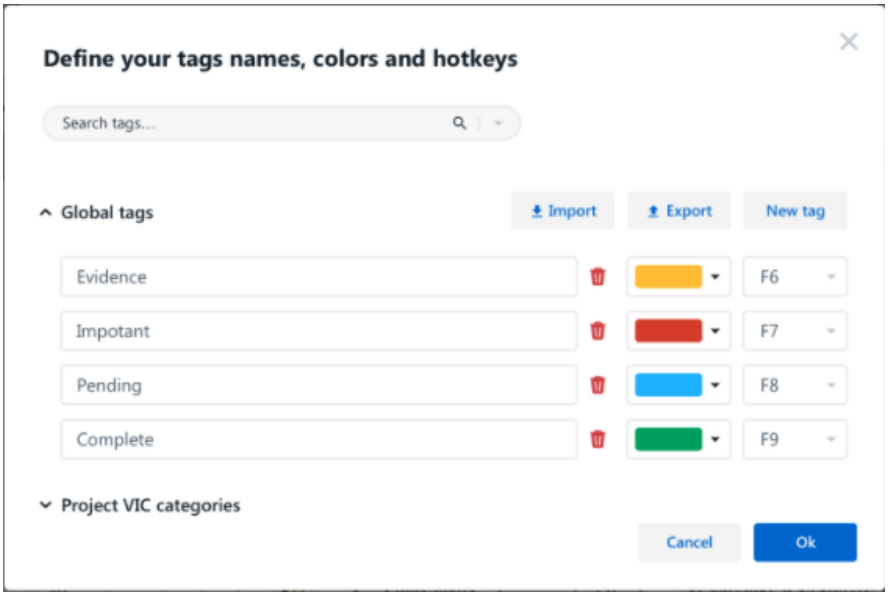
To remove a tag, click .

The tags you create can be viewed via the **Tags** tree item. The number of tags in the project is shown in brackets next to the section name. You can create or remove multiple tags.

Double-click the **Tags** tree item to list the tags in a tab in the data display area. Selected tags are included in reports that you generate.

To manage tags:

1. Click . The following window appears.



> The window also includes Project VIC or CAID categories. For more information, see Importing and categorizing hash sets (on page 152).

2. Define each tag's name, color, and HotKey, as desired.
3. To delete a tag, click 🗑 next to the tag name.
4. To create a new tag, click **New tag**. A new line appears.
5. To export tags click **Export** a list of tag labels.
6. To import tags click **Import** a list of tag labels.

6.11. Device locations

In Physical Analyzer, location data is drawn from different locations within the device. The following location data is analyzed:

Analyzed data > Location related

Location data in the **Locations** item is divided into the following categories:

- Cell towers
- WiFi networks
- Harvested Cell towers
- Harvested WiFi networks
- Media locations
- Favorites
- Reminders
- Home
- Entered
- TomTom
- Foursquare
- GpsFix
- Recent
- Frequent
- Wireless networks

Harvested and non-harvested location information

Harvested and non-harvested location information is taken from the device database.

The device location is identified by the device's GPS information, which is calculated in two ways:

1. Collection - As the device changes locations when traveling with its owner, it collects the location information of each cell tower and Wi-Fi Network Receptor as it enters their vicinity. These locations are called "harvested" information. The location calculated in this way is considered accurate.

   When the device's Wi-Fi is turned on, the device periodically sends the harvested locations to Apple (iPhone devices) or Google (Android devices). The harvested information is then deleted from the device.

   When the device Wi-Fi is turned off, or there is no Wi-Fi connection available, the device harvests and stores the locations of the cell towers and Wi-Fi networks, and then sends the information when the Wi-Fi is turned on, or connection is available.

2. Download - The device connects to the location services provider (Apple (iPhone devices) or Google (Android devices), requesting location services. Apple or Google send information about cell tower and Wi-Fi networks in a ~2km radius. This information is saved on the device and is called "non-harvested" information.

Location data in the Cell towers, WiFi networks, Harvested Cell towers, and Harvested WiFi networks categories includes:

- GPS information - longitude and latitude
- Accuracy - radius in meters within which the device is located.
- Confidence - in %. How confident the service provider is that the phone indeed lies in the calculated location.
- Timestamp

Media locations

Location data in **Media locations** is taken from the location stamp associated with each media file.

Analyzed data > Journeys

Location data in the **Journeys** item is taken from the GPS applications on the device. The categories displayed in this item are divided by application.

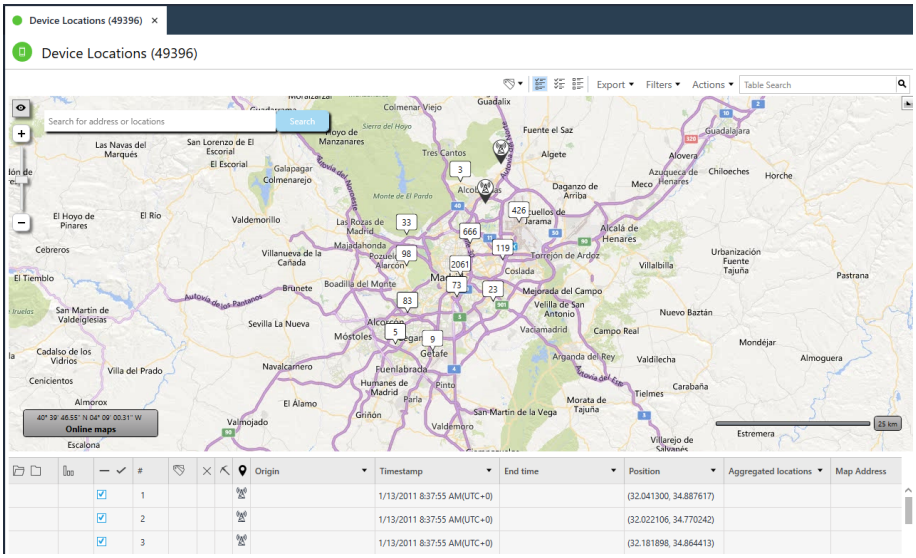
Analyzed data > GPS fixes

Location data in the **GPS fixes** item is taken from GPS devices and GPS applications on the device. The categories displayed in this item are divided by application and source.

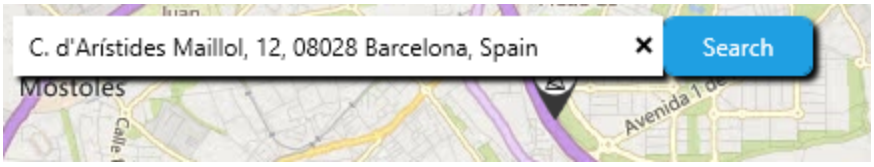
6.11.1. Viewing online maps

The maps function is available to Physical Analyzer users with a valid license. The locations are presented with an icon displaying the location type. Filter the locations based on multiple attributes including date, time and location type.

There are two options: Online maps (which requires Internet access), and Offline maps (see Viewing offline maps (on page 174)). An example of an online map is displayed next.



6.11.1.1. Search and jump to a location on the map



You can use this capability to view all location related events for a specified address. Search for the specific location or zoom-in to the desired location on the map, and all other location related events that occurred in the vicinity will appear on the map. You can search for a location while working in online mode, by typing an address, position (coordinates) or the name of a place.

6.11.1.2. Device origin

The Origin column classifies each recovered location record by its origin: Device or External. You can view and filter for locations that are related and unrelated to the device user's activities. (This does not mean the device has physically been in this location). For example: A picture taken by the camera on a digital device is classified as a Device location. While a picture received on the device is marked as an External location, because the location is related to the image sender. Classified locations are highlighted with a different color on the map.

> Locations that cannot be classified are shown as Blanks i.e., unknown.

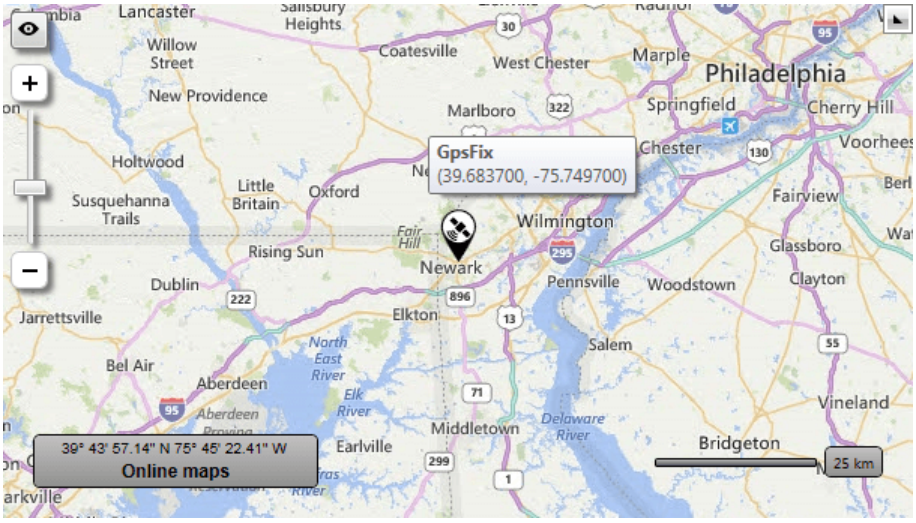
6.11.1.3. Using the map

Users can browse and search topographically-shaded street maps for many cities worldwide. Two types of map views are available to users: Road View and Aerial View.

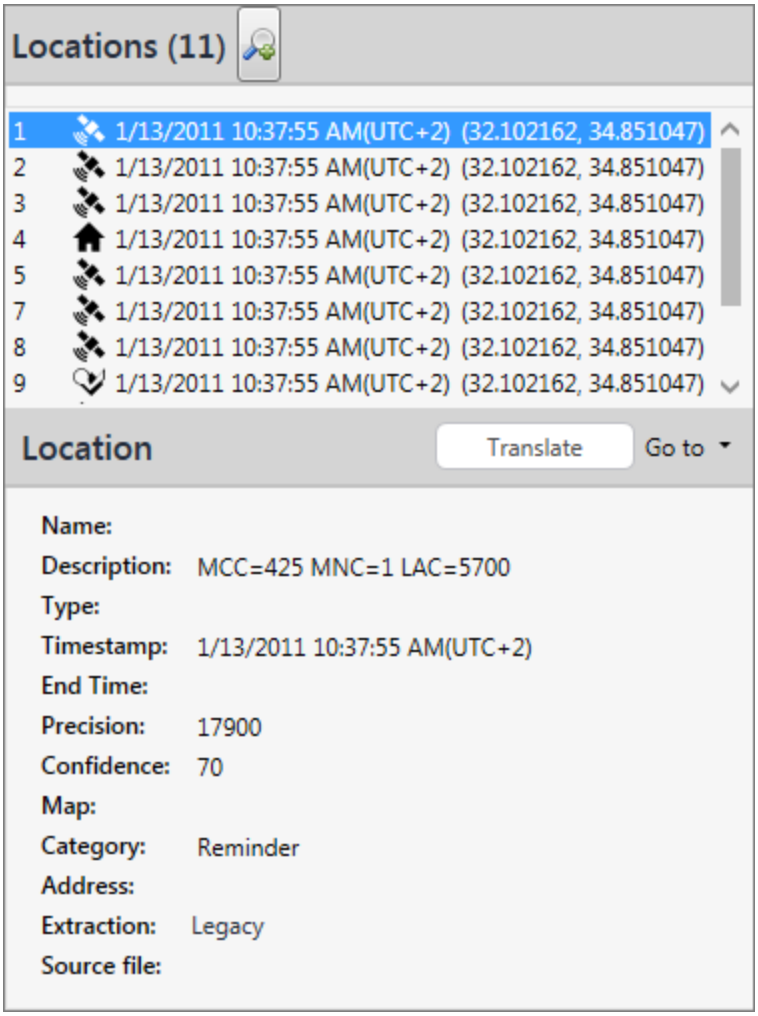
- **Road View:** Road view is the default map view and displays vector imagery of roads, buildings, and geography.
- **Aerial View:** Aerial view overlays satellite imagery onto the map and highlights roads and major landmarks for easy identification amongst the satellite images.

To highlight locations in the table:

- Click or zoom in to a location on the map.



Related events are displayed on the right pane under Locations.



To jump or link to the timeline:

» Click **Go to** on the right pane and select **Timeline**.

A new Timeline tab appears and the selected location is highlighted in the Table view.

6.11.2. Viewing offline maps

View extracted locations using offline maps even without an Internet connection. The maps package installation is required and it is available to Physical Analyzer users with a valid license.

The maps package can loaded to a single installation, or saved to a shared location to which multiple users can connect.

You can choose to use online or offline maps when accessing the device location under Analyzed data.

To change the default map view:

1. Go to **Settings** > **General settings** > **Map** section.
2. Select the desired maps view (**Use online maps** or **use offline maps**).

> The offline maps feature uses a light Windows service that opens and listens to TCP port 3000. To use this feature, you need to select the **Install offline maps service** check box during the Physical Analyzer installation process. If this service was not selected, then you need to reinstall the application.

To download the offline maps package:

1. Login to MyCellebrite.
2. In **Products and Licenses**, click in the Physical Analyzer product box.
3. In **Maps Pack**, locate and download the Offline maps package.

> There are a number of offline map packages. You can view extracted locations on a worldwide map, and zoom in at a higher resolution to view streets in selected continents using offline maps.

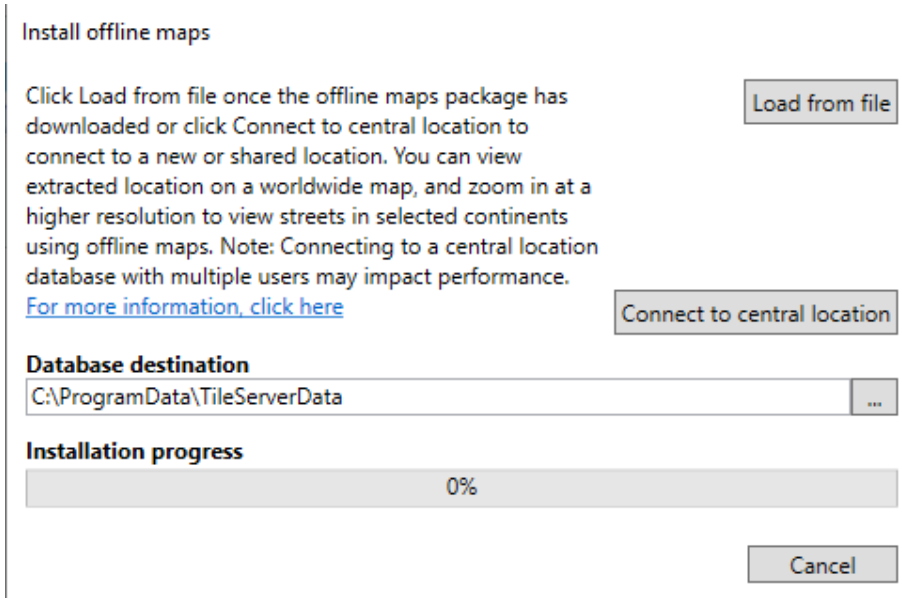
> The **Offline maps - Worldwide** package must be downloaded and installed before installing a regional offline maps package.

> To reduce merge processing time when working with a shared location, it is recommended that only the user that has the offline maps on their machine will install new maps. Other users can still connect to the offline maps.

> Merge processing time also depends on network issues and how busy the central machine is when downloading.

To install the offline maps package:

1. After downloading the relevant offline maps package, in Physical Analyzer, go to **Tools** > **Offline maps** > **Install Offline maps Package**. The following window appears.

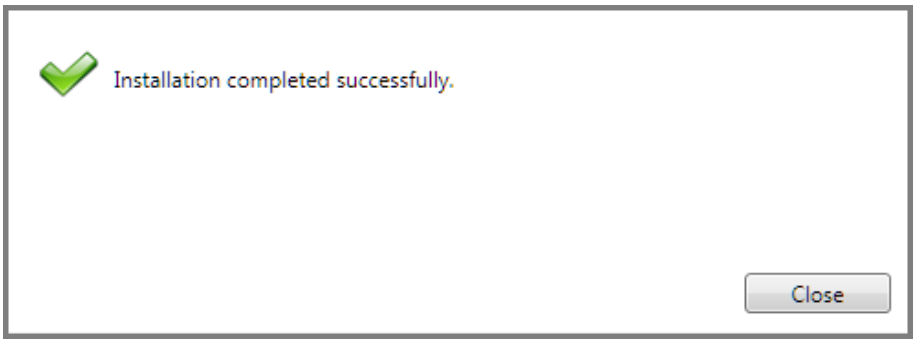


> Click ... to change the default location where the offline maps are installed.

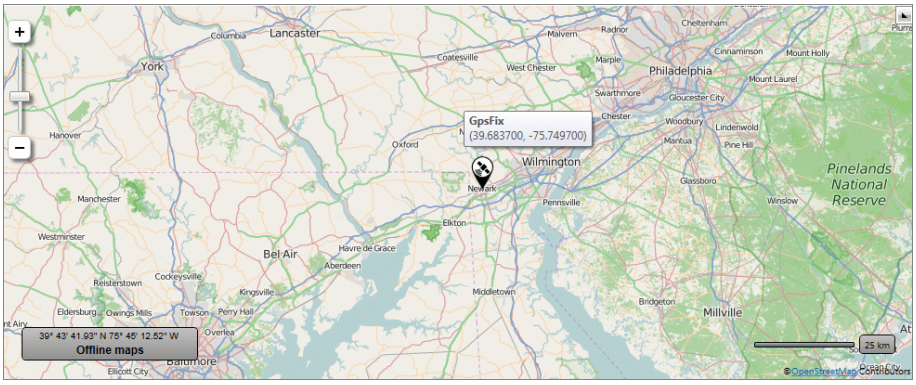
2. Select one of the following options:
   - Click **Load from file** to load the offline maps package. Due to the size of the file, the loading process takes some time to complete.
   - Click **Connect to central location** to connect to a shared location where the offline maps package has been saved.

> Connecting to a central location database with multiple users may impact performance

3. The following window appears:



The offline maps are now installed and ready to use. An example of an offline map is displayed next.



6.11.3. Markers and information windows

Markers signify the location where a person's device registered.

The color of the marker signifies which person was registered at a particular location. At a low zoom level, markers show the approximate location, and may include the data of more than one person.

The following markers are examples of the types of markers that are displayed in the map:

At low zoom level, this marker displays a number of recorded locations in a particular area.

Indicates the location of the cell tower that registered the person's device.

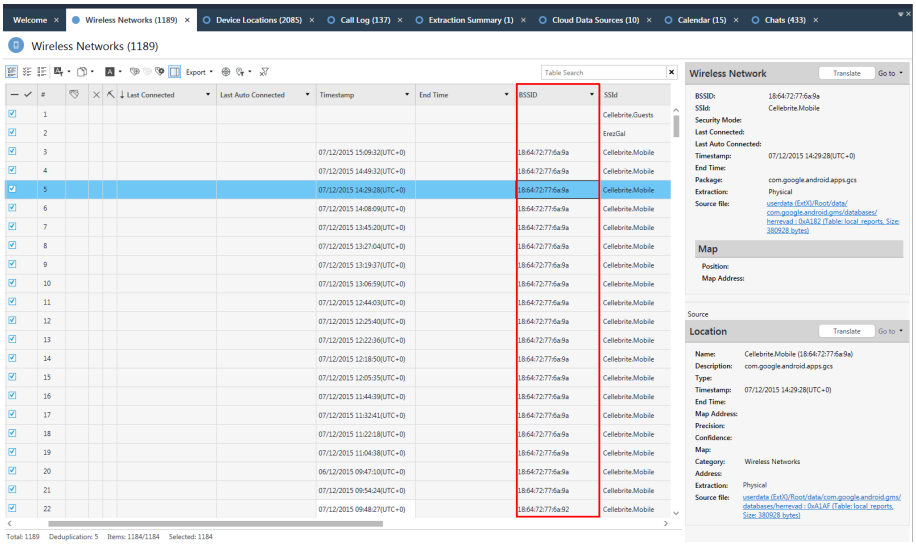
Indicates the location of the WiFi network receptor that registered the person's device.

Indicates the recorded location or a media object.

Indicates the location of an unidentified entity that registered the person's device.

6.11.4. Enrichment of BSSID and cell IDs

Physical Analyzer enables you to enrich the location data recovered from mobile devices by converting BSSID (wireless network) and cell IDs (cell tower) to physical locations. When viewing location data, BSSID values are displayed. An example is displayed next.

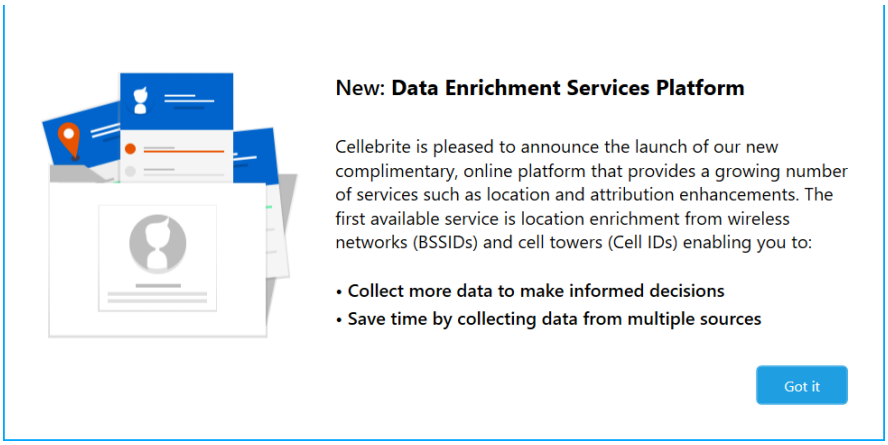


> If all BSSIDs/cell IDs have already been enriched, then the Enrichment feature is not available.

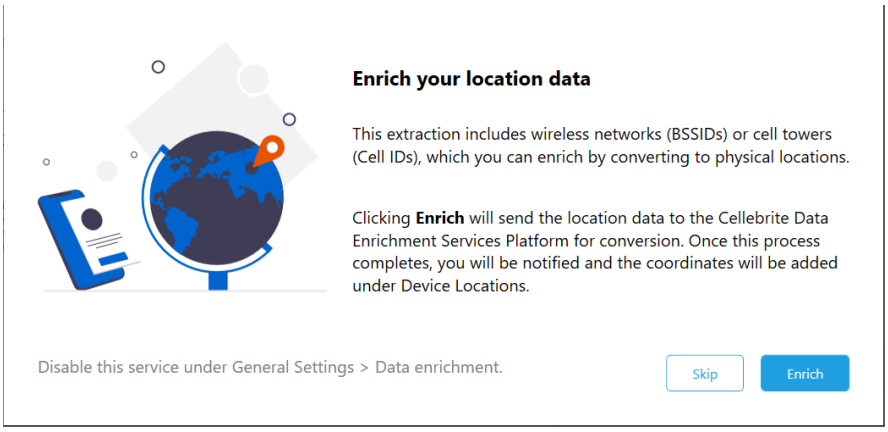
6.11.4.1. Online enrichment

To enrich BSSID and cell tower IDs (online):

1. If you have an Internet connection and you open an extraction with BSSID or cell IDs, the following window appears (the first time only).



2. Click **Got it**. The following window appears.



3. Click **Enrich** to convert to the physical locations via the Enrichment service.

> You will receive a notification when the process completes and the new locations will be added under **Device Locations**.

> You can also access **Online enrichment** from **Tools** > **Enrichment of BSSIDs and Cell IDs**.

6.11.4.2. Offline enrichment

To start using the BSSID feature, first download the database. This is an offline solution and does not require an Internet connection.

To download the BSSID database:

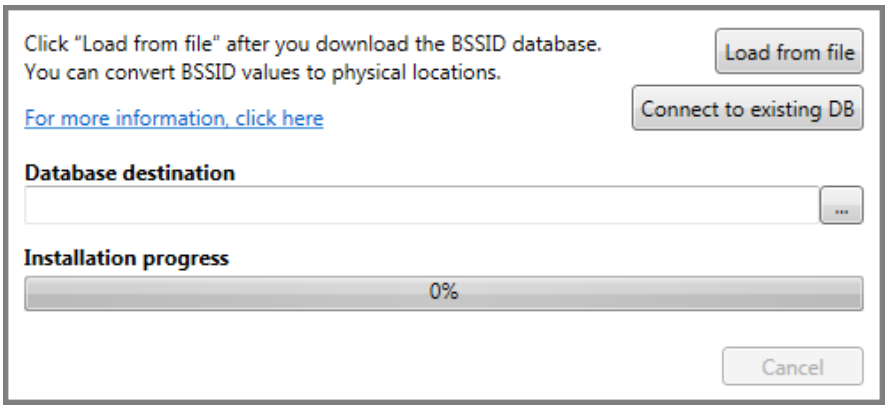
1. Login to MyCellebrite.
2. Click the **Downloads** tab.
3. Download the BSSID database. Make note of the location.

> To aid the download process, you can optionally download split database files (10 files, 6 GB file size) and load these files into Physical Analyzer. These files will be merged into a single database file, but the files must all be located together. When you load the split files, you need to select the main (or first) database file.

> You can save the database to a network location for use by multiple users.

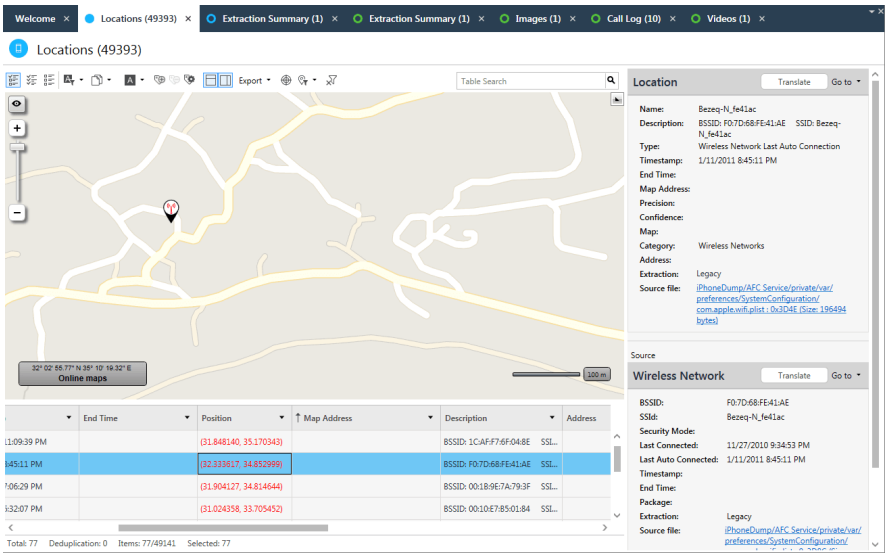
To install the BSSID database:

1. From the **Tools** menu, select **Enrichment of BSSID and cell IDs** and click **Install**. The following window appears.



2. Click **Load from file** to use the database on your computer or **Connect to existing DB** to use a database saved on your network.
3. Navigate to the location of the database and click **Open**. The database is installed.

   Once the BSSID database is installed, Physical Analyzer converts the BSSID values to physical locations. An example is displayed next.



To enrich BSSID and cell tower IDs that are not in the database:

1. Select **Tools > Enrichment of BSSID and Cell IDs > Export** to generate an XML report with unenriched BSSID and cell tower values.
2. Email the report to enrichment@cellebrite.com.
3. You will receive an enriched report with converted positions via email.
4. Select **Tools > Enrichment of BSSID and Cell IDs > Import** to import the enriched report to the current project.

To disable the automatic conversion of BSSID and cell tower IDs to physical locations:

1. From the **Tools** menu, click **Settings**.
2. Under **General settings**, scroll down to **Data enrichment**.
3. Clear the **Convert BSSID values (wireless network) to physical locations** check box.

6.11.5. Retrieving addresses

You can view street addresses for longitude and latitude positions extracted from a device. This can then be used to filter the locations. You can select single or multiple locations up to a maximum of 1,000. You can retrieve street addresses in the following views: Project search, Timeline views and Watch List results.

> To use this feature, you must be connected to the Internet.

To retrieve an address:

» In one of the Device locations table views, select a row, right-click and select **Retrieve address**, or click **Actions > Retrieve address.**

> To retrieve multiple addresses, you can use Ctrl button to select the locations. You can retrieve a maximum of 1,000 items.

	External	8/9/2017 2:23:19 PM(UTC+0)	(32.101636, 34.850678)	49000 Petah Tik
	External	8/9/2017 2:21:58 PM(UTC+0)	(37.827580, -122.4818...	Golden Gate Bridge, Sausalito, CA 94965
	External	8/9/2017 2:21:37 PM(UTC+0)	(37.827580, -122.4818...	Golden Gate Bridge, Sausalito, CA 94965
	External	8/9/2017 3:21:37 PM(UTC+0)	(37.827580, -122.4818...	Golden Gate Bridge, Sausalito, CA 94965
	External	8/9/2017 4:21:37 PM(UTC+0)	(37.827580, -122.4818...	Golden Gate Bridge, Sausalito, CA 94965

The retrieved addresses are displayed in blue in the column called Map Address.

To filter locations:

» Click **Filters > Location** and then select one of the following options:

- » **Show All** to display all locations.
- » **With map address** to display only locations that have a map address.
- » **Without map address** to display only locations that do not have a map address.

> Enriched data will appear in blue indicating this is enriched data from Cellebrite and didn't come from the device.

6.11.6. Decoding and analyzing drone data

Drones are becoming more and more involved in crimes including smuggling, carrying weapons and even threats to passenger aircraft. Physical Analyzer provides decoding of intact and deleted data from popular drone models.

Supported data artifacts include: Media files, metadata, locations and timestamps, home points, elevation, drone identifiers, and deleted data including deleted journeys and home points (data that was automatically deleted by the drone).

6.11.6.1. Drone flight path

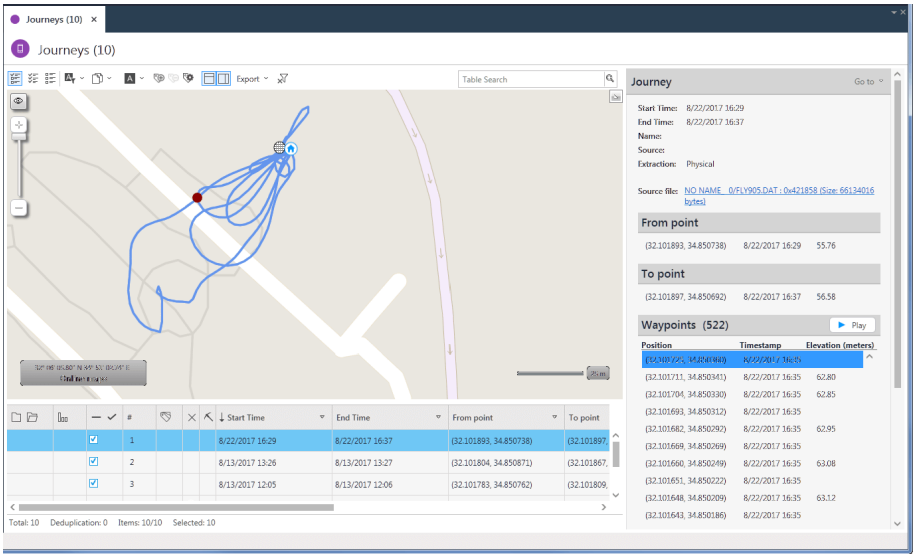
Each drone flight has its own journey with positions. The positions are presented on a map with a flight path, and you can play and visually track the drone's flight.

To view the drone's flight path:

1. Under **Analyzed Data** > **Device Locations** > double-click **Journeys**.

   The symbol on the map indicates a drone's flight path. Hover over this symbol to see the From point with GPS details including: date, time, longitude, latitude, and elevation in meters.

2. In the right pane, in the Waypoints area, click the **Play** button to simulate the drone's flight. Click the **Stop** button to end the simulation. The symbol on the map indicates the To point.
3. Click a waypoint in the list to indicate its position with a red circle on the drone's flight path. An example flight path is displayed next:



The right pane includes the following information:

- **Journey information:** Start time, end time, app name of the drone for this particular journey (the user may have more than one drone), source, type of extraction (i.e., Physical extraction), and source file.
- **From/To points:** Longitude, latitude, start date and time, and elevation from sea level in meters.
- **Waypoints:** A selection of some of the waypoints from the drone's flight path including position, timestamp and elevation.

> The **Play** button is not displayed if there are more than 50 meters between waypoints, because this could indicate that the drone's flight path is not valid.

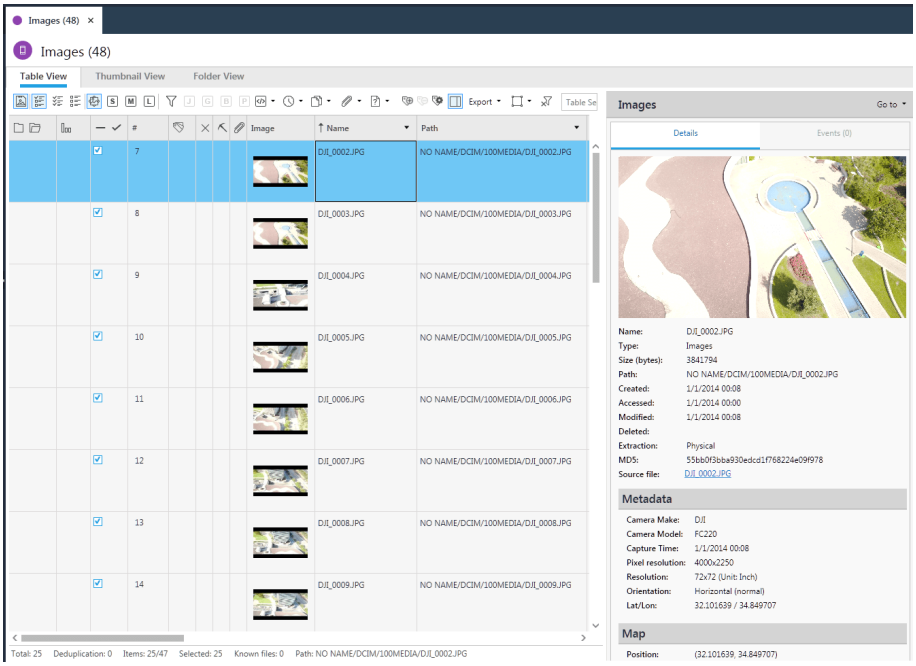
6.11.6.2. Images/videos

Images and videos files taken by the drone during flights. Images and videos are displayed under **Analyzed Data** > **Media Images** > **Images / Videos**.

This right pane includes the following information:

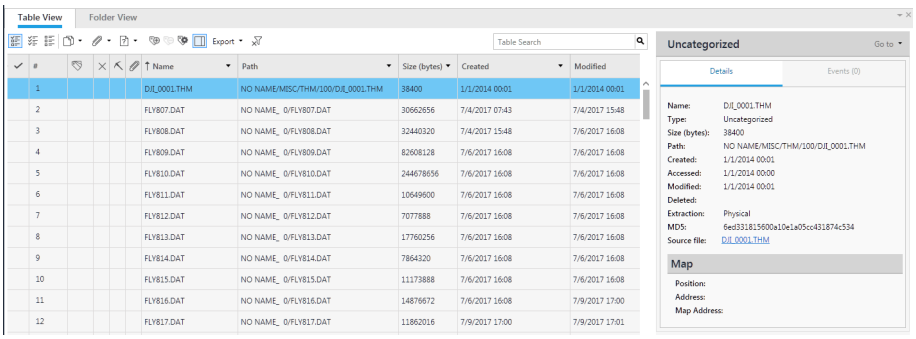
- **Details:** Image name, type (Images or Videos), size, path, creation date, accessed date, modified date, whether it resides in deleted data, type of extraction, MD5, and source file name.
- **Metadata (EXIF):** Make of camera, Camera model, capture time, pixel resolution, image resolution, orientation, latitude, and longitude.
- **Map:** position of the drone on the map, as well as any physical address and map address.

An example is displayed next:



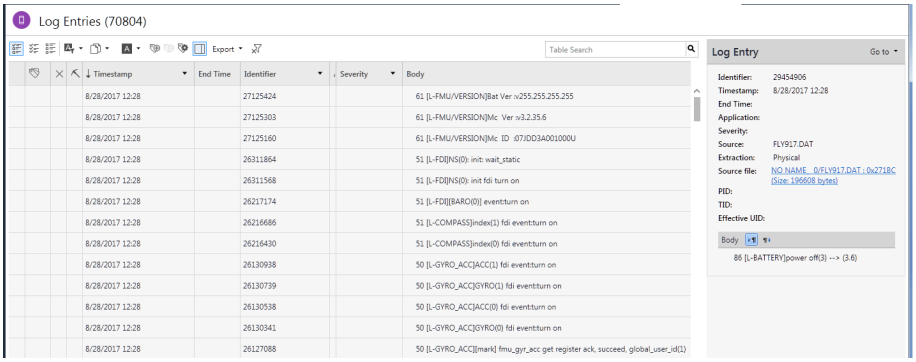
6.11.6.3. Log files

The drones log files are located under **Data Files** > **Uncategorized**. An example is displayed next:



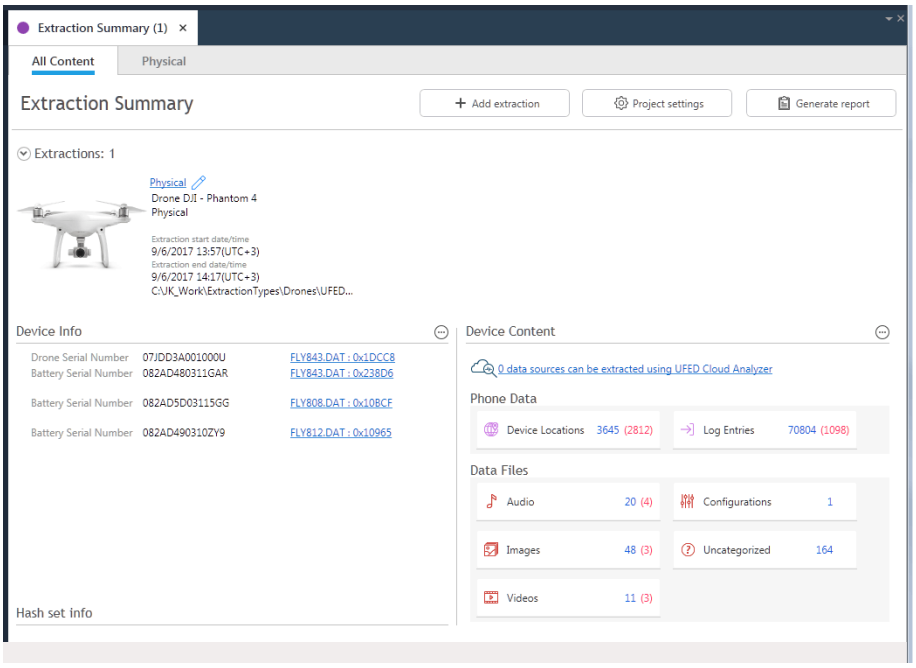
6.11.6.4. Log entries

Log entries that were written to the drone's log file under **Analyzed Data** > **Log Entries**. An example is shown next:



6.11.6.5. Device info

The Extraction Summary displays information about the drone model, when the extraction was performed, drone serial number and battery serial numbers. The drone serial number is the recovered serial number from the drone's log files. This number may be different from the serial number that appears on the actual drone. The serial number of the battery could be the current battery or a previous battery. An example is shown next:



6.12. Recording screen captures and video

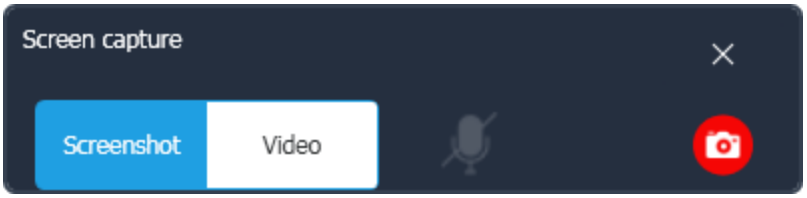
Use the Capture tool to record screen captures and videos. This enables you to quickly and clearly document and explain your digital investigative processes, build visual reports that are easy to present and share, and communicate with other personnel more effectively.

For each screen capture or video recording, you can select an area, enter a label, add notes, save to a project or location on your computer, and include it in a report. The screen captures and videos can be included in all report formats including UFDR files, which can then be presented in Cellebrite Reader.

> To use the Capture tool and play video playback, you need Windows Media Player (default version for installed OS or higher).

To perform a screen capture or video recording:

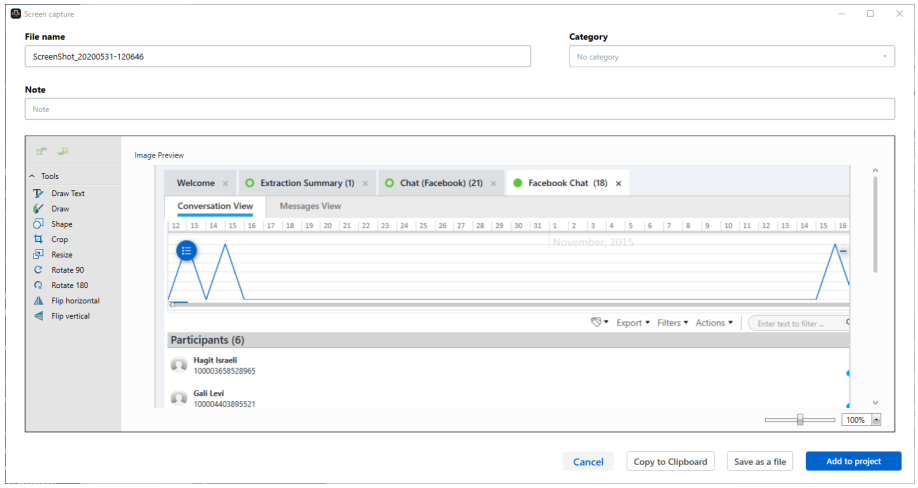
1. Click **Screen capture** ( ). The screen capture window appears.



2. Select **Screenshot** or **Video**.

6.12.1. Screenshot

1. Click **Capture** ( ).
2. Select the capture area. The screenshot is taken and the following window appears.

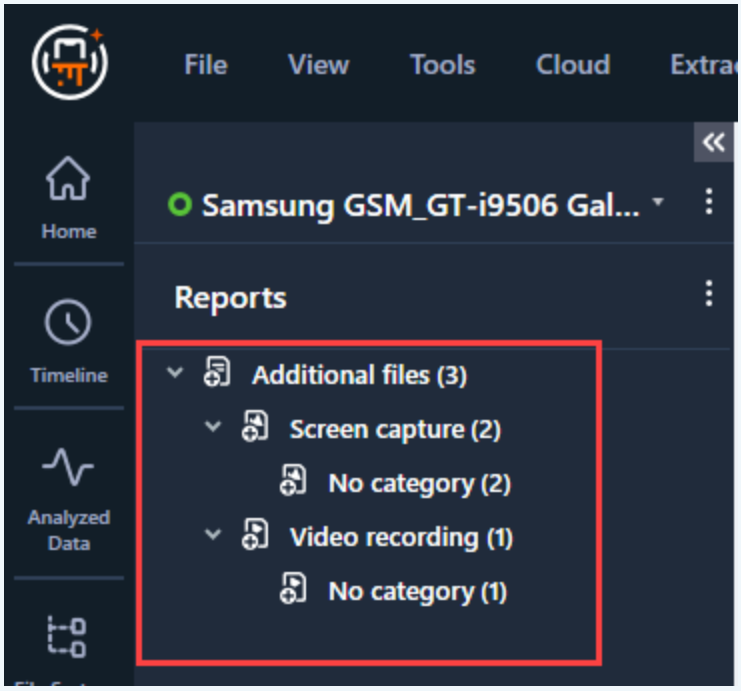


3. Use the default file name or enter a new name.

> You cannot use the same file name that exists in another open project.

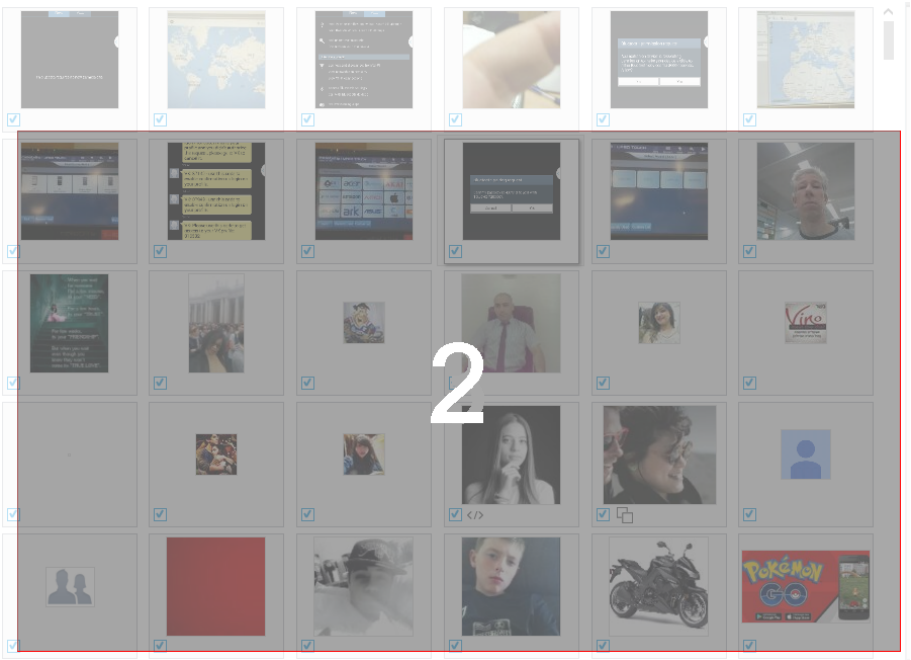
4. Select a category or enter a new category. The system remembers a maximum of 10 categories. The default category is "No category". The screen capture is displayed under the selected category in the project tree.
5. Enter any notes to describe the screen capture.
6. If required, you can use the Tools on the left to add text, draw shapes, crop, resize, rotate, or flip the screen capture.
7. Click **Copy to Clipboard** to copy the screenshot, click **Save as a file** to save the screenshot to your computer (or network location), or **Add to project** to add the screenshot to a specific Physical Analyzer project.

Screenshots and videos are added to the Reports view project tree under **Additional files**.



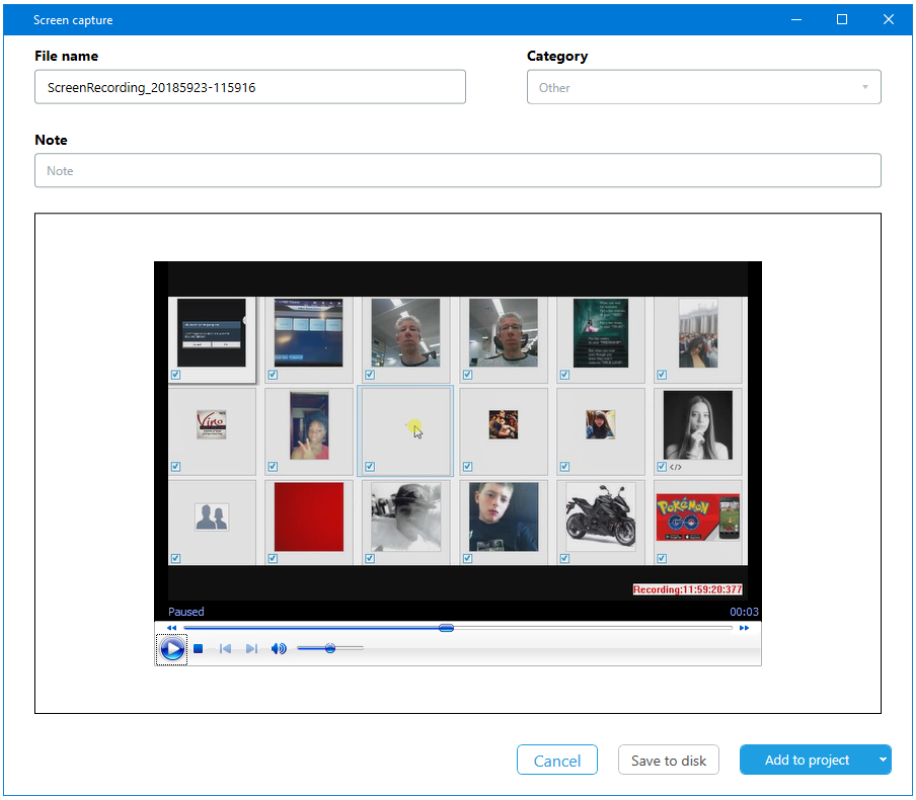
6.12.2. Video

1. Enable or disable the microphone ( ).
2. Click **Capture** ( ).
3. Select the capture area. The video recording begins.



4. Perform the relevant actions that you want to record.

5. When you've finished, click **Stop** ( ) or **Pause** ( ). The following window appears.



6. Use the default file name or enter a new name.

> You cannot use the same file name that exists in another open project.

7. Select a category or enter a new category. The system remembers a maximum of 10 categories. The default category is "No category". The video is displayed under the selected category in the project tree.
8. Enter any notes to describe the video.
9. Click **Save as a file** to save the video to your computer (or network location) or **Add to project** to add the video to a specific Physical Analyzer project.

> Videos can be a maximum two hours long.

7. Translating decoded data

Translate the content in extractions that are in foreign languages without having to wait for a translator to become available, or to use Internet-based tools. The Translation feature enables investigators to translate decoded data on demand. It is an offline translation solution, where you do not need to be connected to the Internet. You can select single, multiple or all table entries for translation. Both the original and the translated text can be included in reports.

The Translation feature includes two different options:

- Smart Translator (below)
- Basic translation pack (on page 197)

> Contact Cellebrite Sales to include the Translation feature and the required language options in the Physical Analyzer license.

7.1. Smart Translator

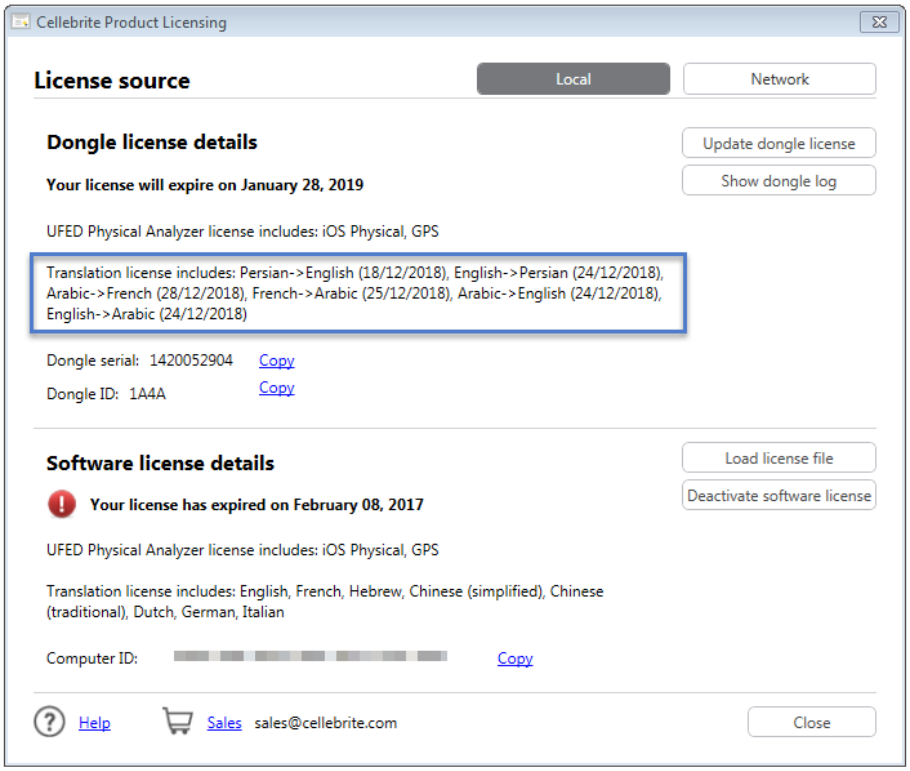
Translate even more decoded data with the Smart Translator, supporting a comprehensive range of requested languages. Smart Translator languages includes additional languages that are not part of the Basic transaction pack including: Arabic, Arabizi, Persian, Turkish, Romanian, Pashto, Vietnamese and Swedish. To use the Smart Translator languages, you need to select language pairs. Each language pair is license separately. Contact Cellebrite Sales to include the Smart Translator languages in the Physical Analyzer license.

To upload the dongle license key:

1. Click **Help** > **Show license details**. The Cellebrite Product Licensing window appears.
2. Click **Update dongle license** and load the license key that includes Smart Translator languages.

> Before you can use the Smart Translator, you *must* upload the dongle license key.

An example license with the Smart Translator translation languages is displayed next.



For a list of the latest supported langauges refer to www.cellebrite.com

Smart Translator languages are only applicable to dongle licenses.

If you move a dongle license to another computer, you will need to install the Smart Translator languages again.

Text with multiple languages will not be fully translated.

Each SDL language engine consumes ~ 1 GB memory (RAM).

To use the Smart Translator:

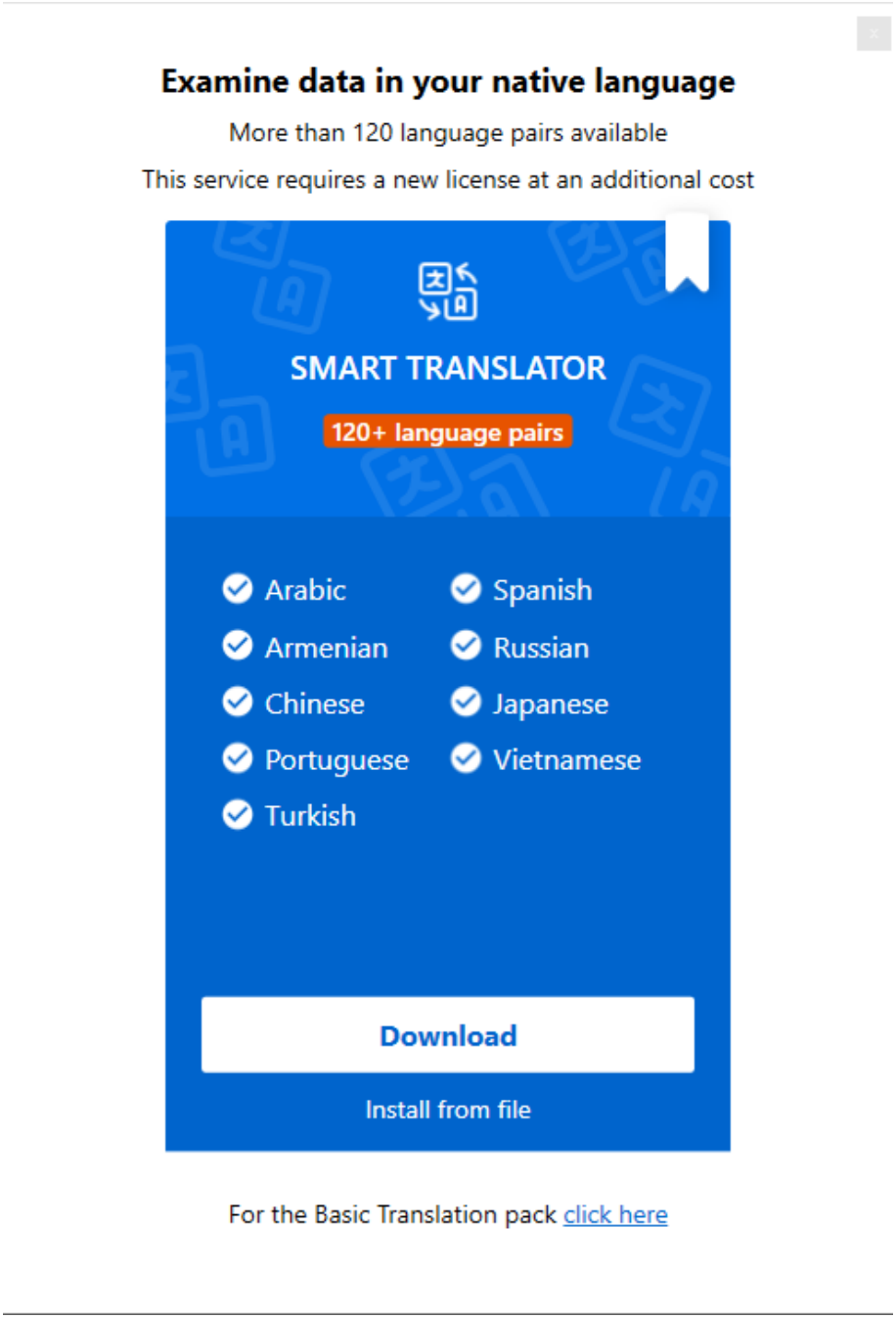
» Installing the Smart Translator languages (below)

7.1.1. Installing the Smart Translator languages

You can download the Smart Translator languages from the application or your MyCellebrite account. Multiple languages can be selected, but each language needs to be installed separately.

To install Smart Translator languages:

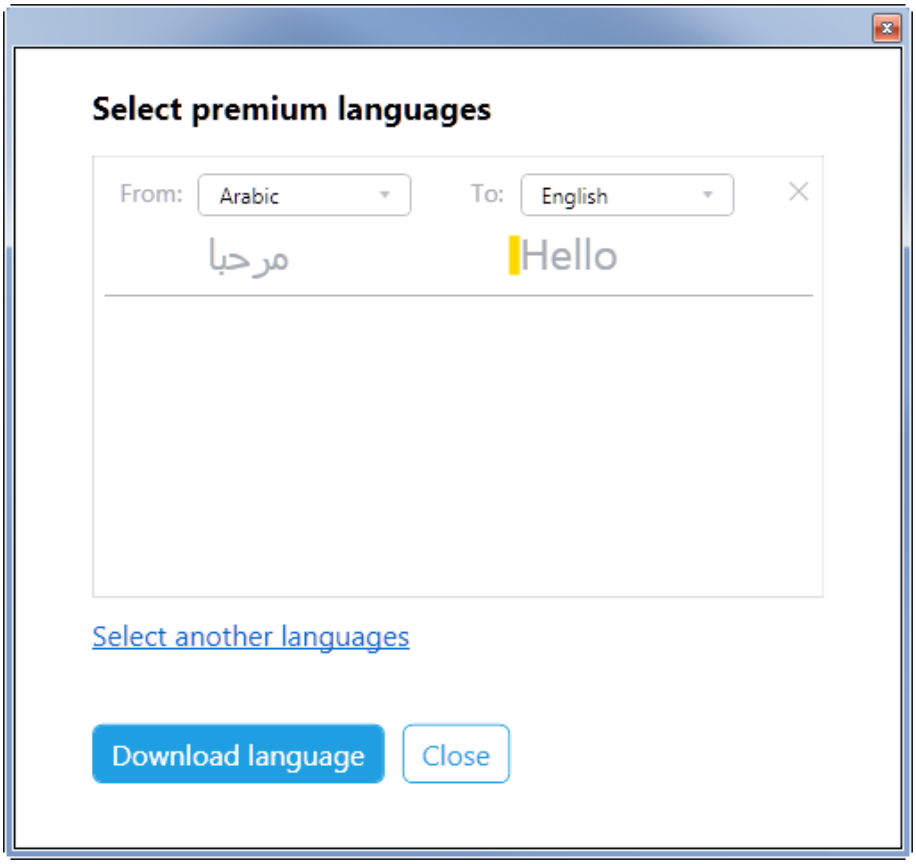
1. Select **Tools** > **Translation**. The following window appears.



2. Select to **Download** or **Install from file**. As explained next.

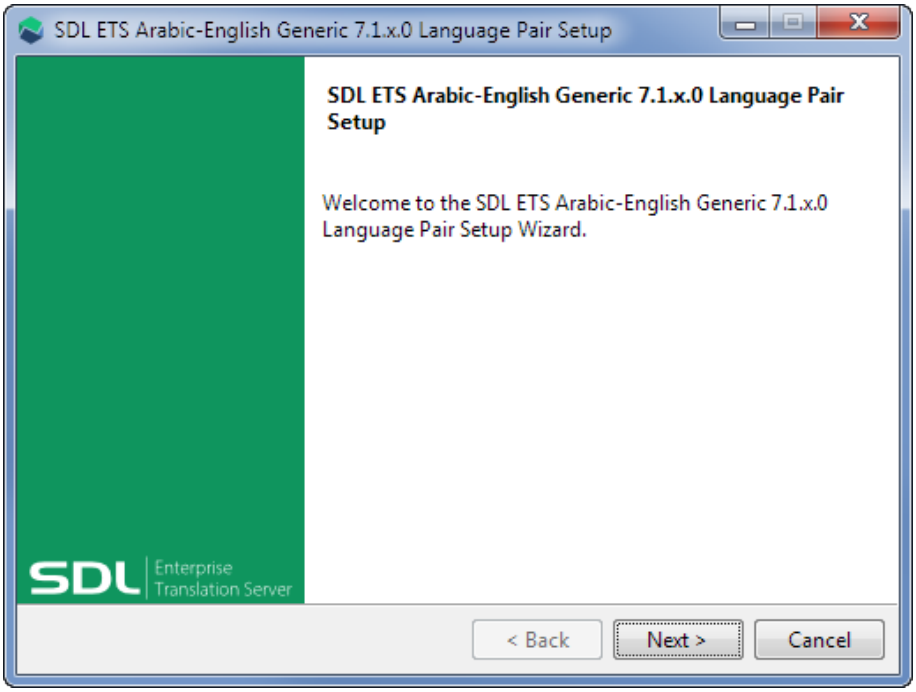
To download the languages:

1. Click **Download** to download the languages from the application. Select this option if you have an Internet connection. The following window appears.

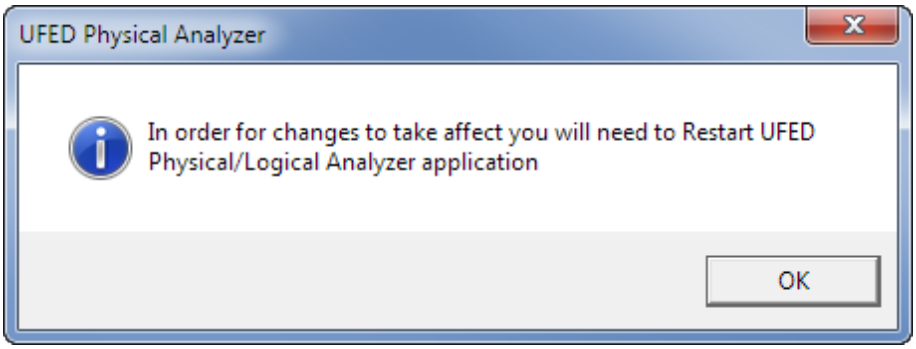


2. Select the required language pair to install.
3. If required, click **Select another language pair** to install additional language pairs. Each language pair is installed separately, therefore the more languages selected the longer the installation process takes. Also, due to the size of the language files, they take time to download.

   When the installation starts, the following setup window appears.



4. Follow the on-screen instructions to install the selected language pair. At the end of the installation process the following window appears:

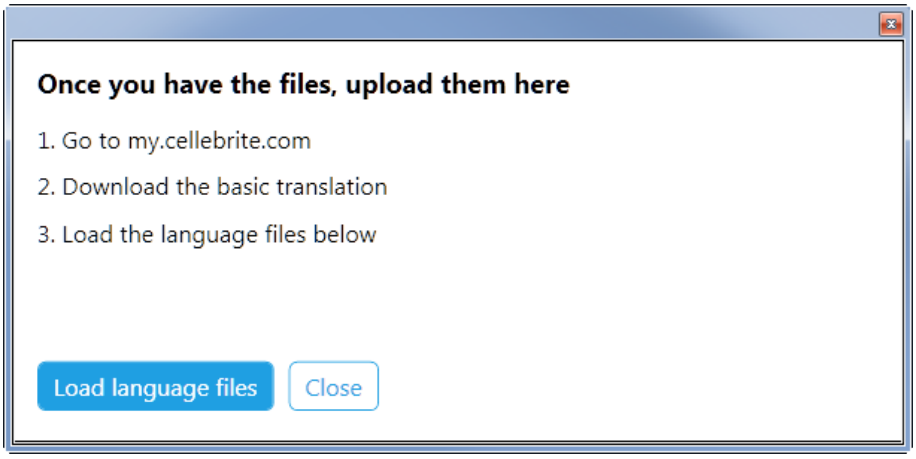


5. Click OK and restart Physical Analyzer.

To install a language pair from a file:

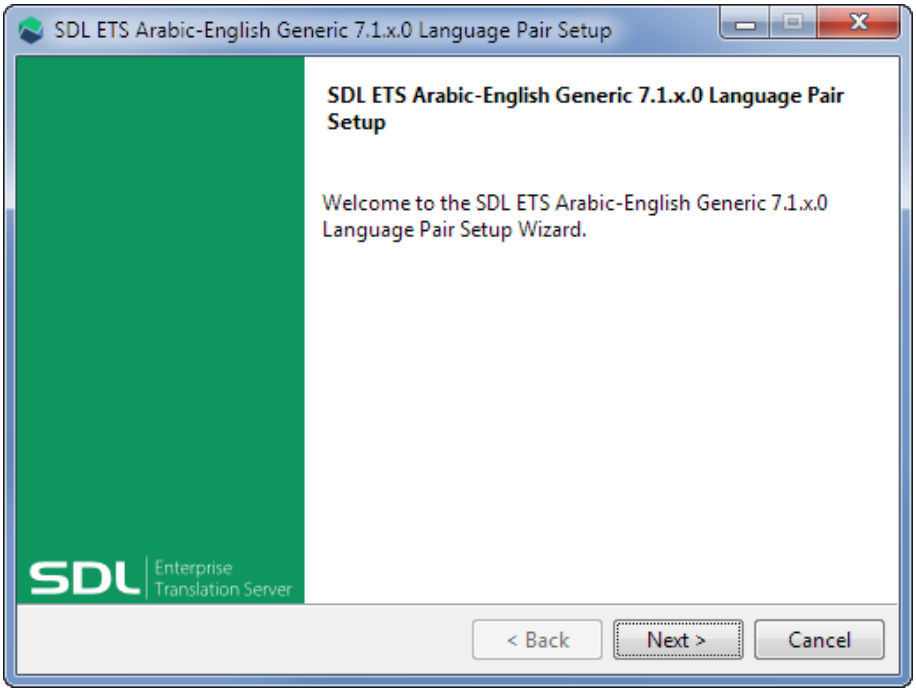
1. Click **Install from file** to install a language pair from a file, which has been downloaded from **MyCellebrite** > **Add-ons**. Select this option if there is no Internet connection, or you have previously downloaded the language pair. There is a file for each language pair.

   The following window appears.

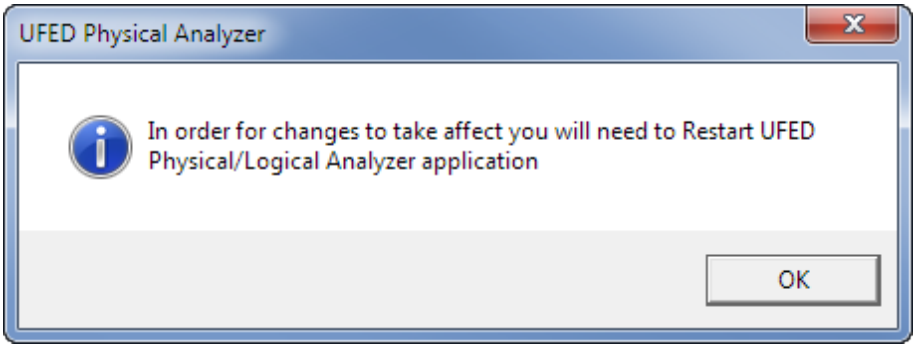


2. Follow the instructions, and then click **Load language files**.
3. Select the required language and then click **Open**.

   When the installation starts, the following setup window appears.



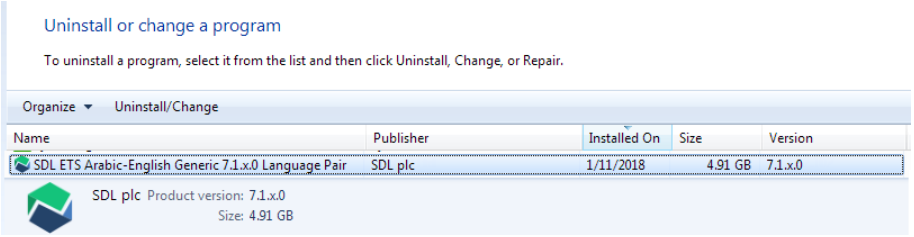
4. Follow the on-screen instructions to install the selected language pair. At the end of the installation process the following window appears:



5. Click OK and restart Physical Analyzer.

7.1.1.1. Uninstalling a language pair

To uninstall the language pair, go to the Windows Uninstall page, and select the SDL ETS Language Pair, (Publisher: SDL plc) from the list.



7.2. Basic translation pack

This pack includes 14 common languages. You can select up to five languages for free, from the My Products page in MyCellebrite. Additional languages are available to be purchased. You cannot change a language after saving, but you can request additional languages. If a required language is not included in the Basic translation pack, you can purchase a Smart Translator language (see Smart Translator (on page 191)).

> If you want to translate to a language other than English, you should select it as well.

The supported languages in the Basic translation pack, are as follows:

Chinese (Simplified)	Japanese (requires additional payment)
Chinese (Traditional)	Korean
Dutch	Polish
German	Portuguese

Hebrew	Russian
Italian	Spanish
French	Ukrainian

Steps to use the Basic translation pack:

- Installing the Basic translation pack (below)
- Selecting the languages in MyCellebrite (on page 202)

7.2.1. Installing the Basic translation pack

You can download the Basic translation pack from the application or your MyCellebrite account. The Basic translation pack includes a version number, which enables you to track the version installed on the computer.

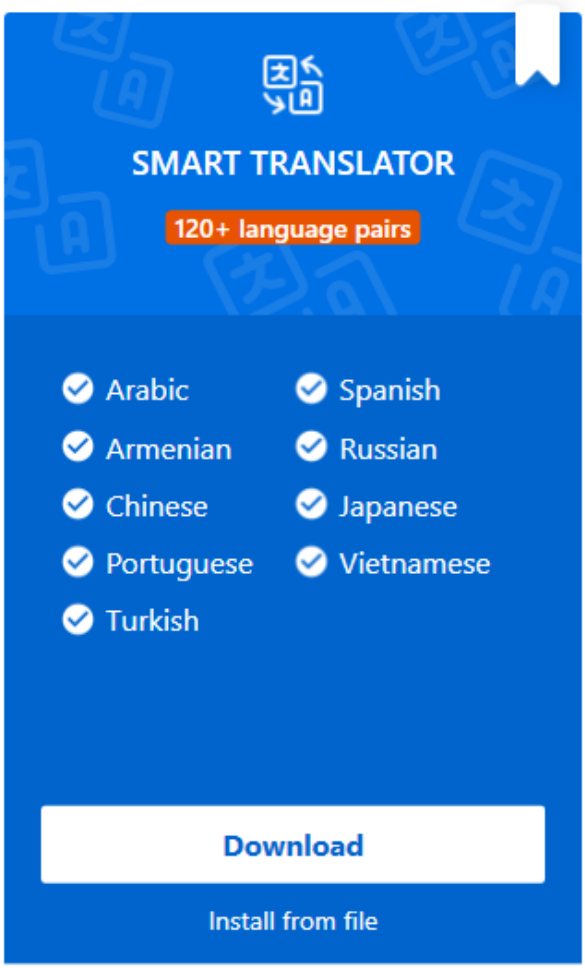
To install the Basic Translation pack:

1. Select **Tools** > **Translation**. The following window appears.

Examine data in your native language

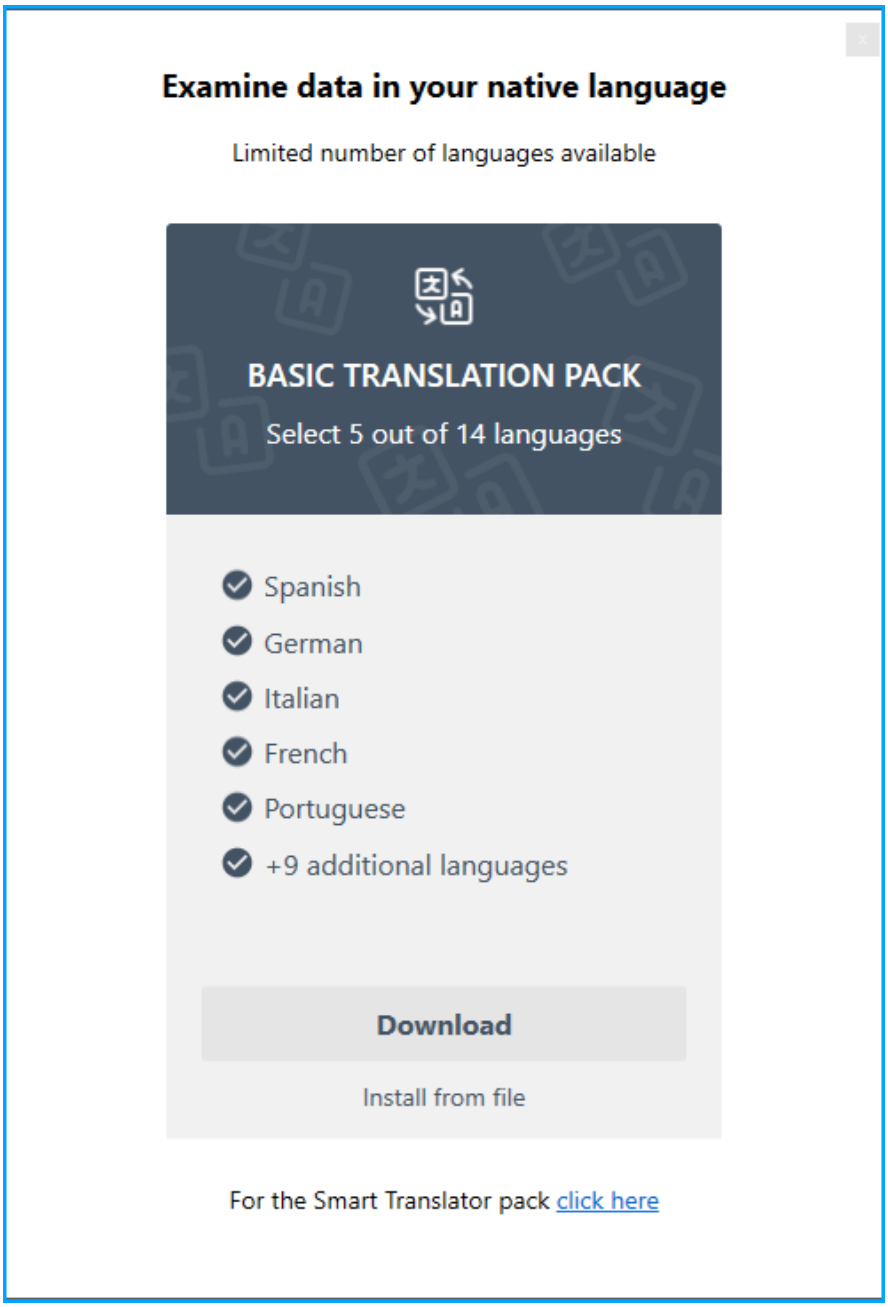
More than 120 language pairs available

This service requires a new license at an additional cost



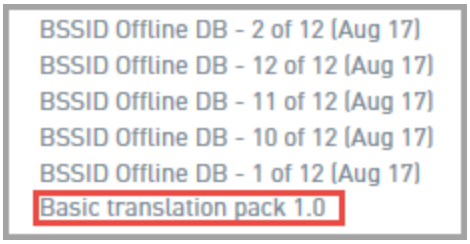
For the Basic Translation pack click here

2. Select the **click here** link to access the Basic Translation pack. The following window appears.

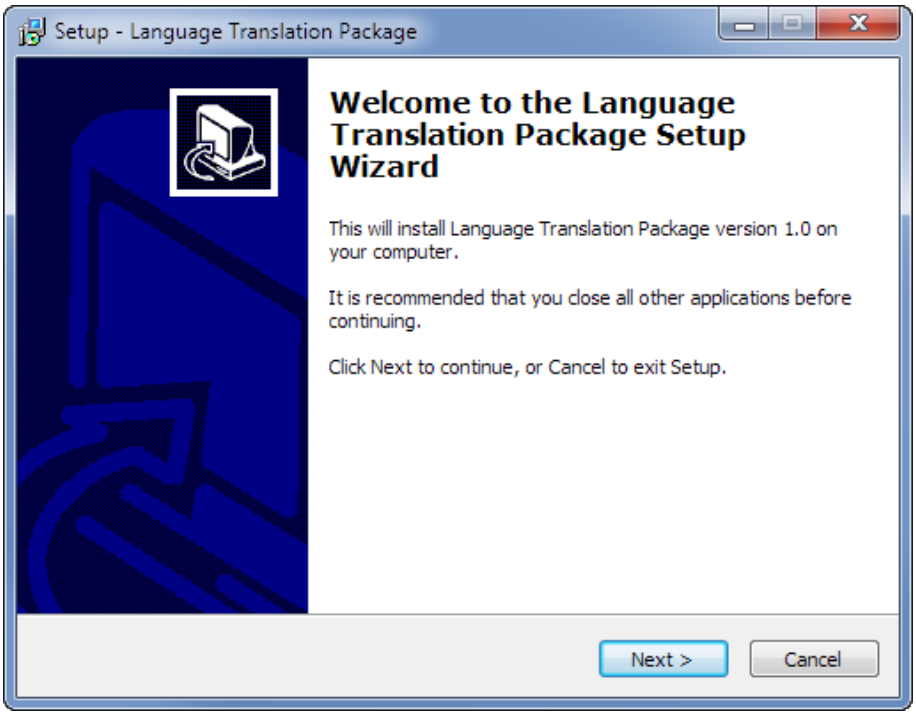


3. Select one of the following options:
   - **Download:** Downloads the Basic translation pack (Internet connection required).
   - **Install from file:** Installs the Basic translation pack from a file, which has been downloaded from **MyCellebrite** > **Add-ons**. The file is called `Basic translation pack 1.0`. Select this option if there is no Internet connection, or you have previously downloaded the pack. An example of the download file from the MyCellebrite page is

displayed next.



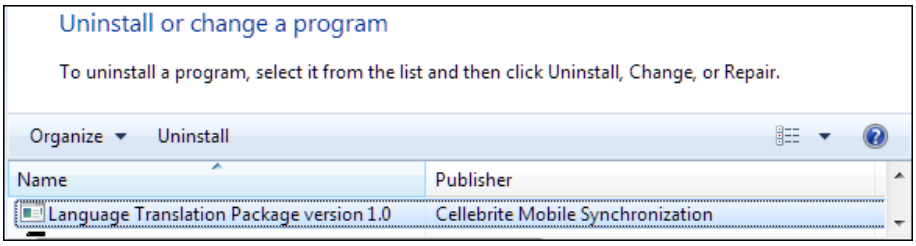
When the installation starts, the Setup window appears.



3. Follow the on-screen instructions to install the Basic translation pack.

7.2.1.1. Uninstalling the Basic translation pack

To uninstall the Basic translation Pack, go to the Windows Uninstall page, and select the Language Translation Package, (Publisher: Cellebrite Mobile Synchronization) from the list.

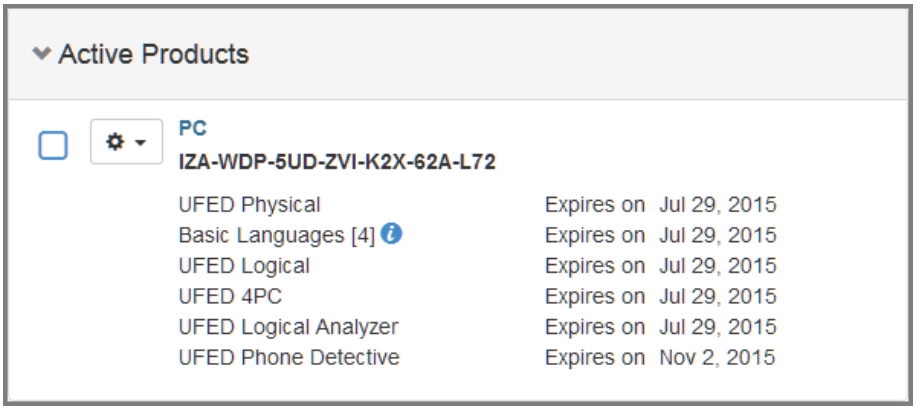


7.2.2. Selecting the languages in MyCellebrite

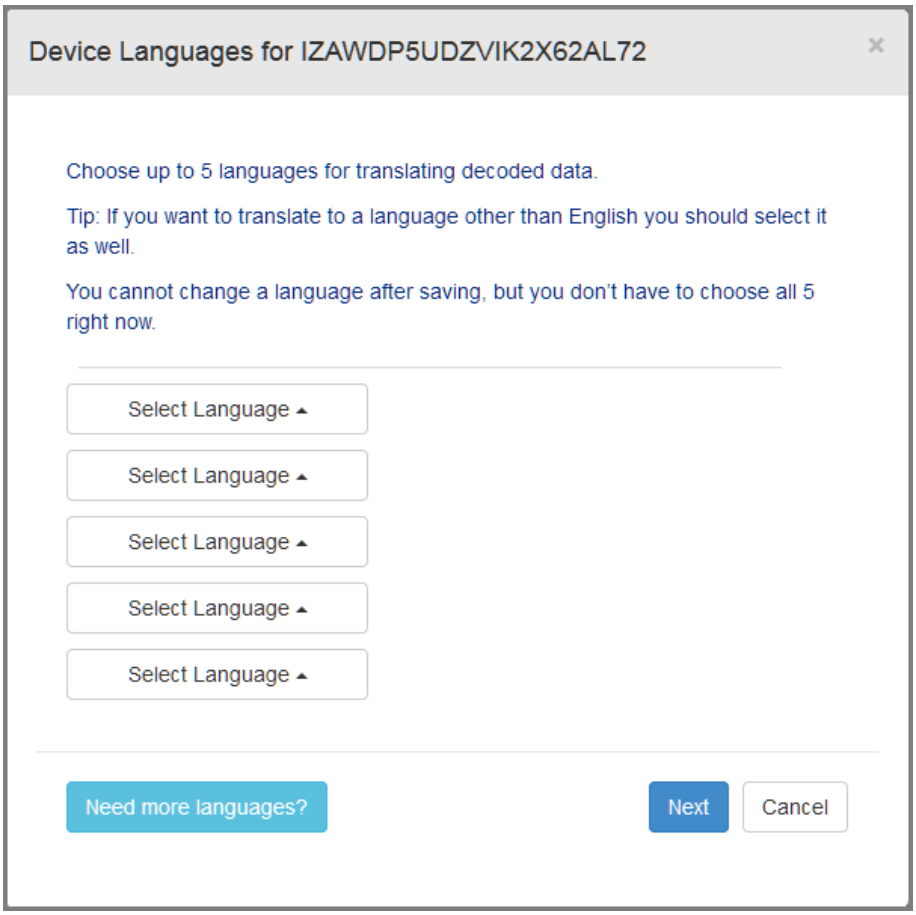
You can select up to five languages for free from the My Products page in MyCellebrite.

To select languages:

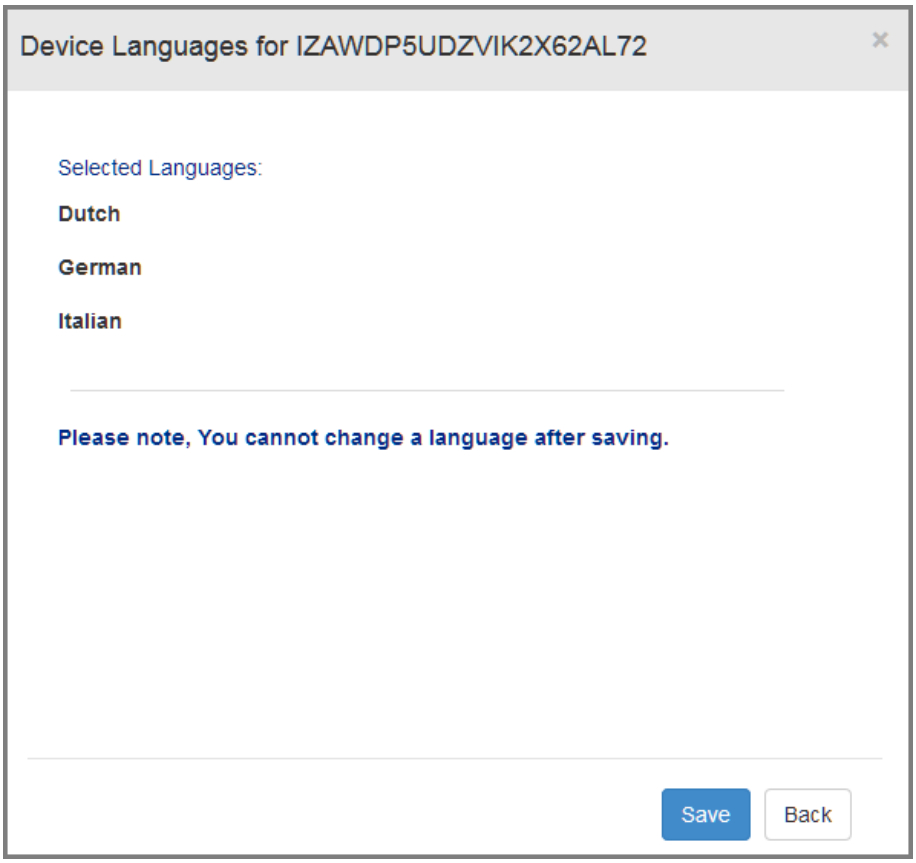
1. Log in to MyCellebrite and select the **My Products** tab. The following window appears.



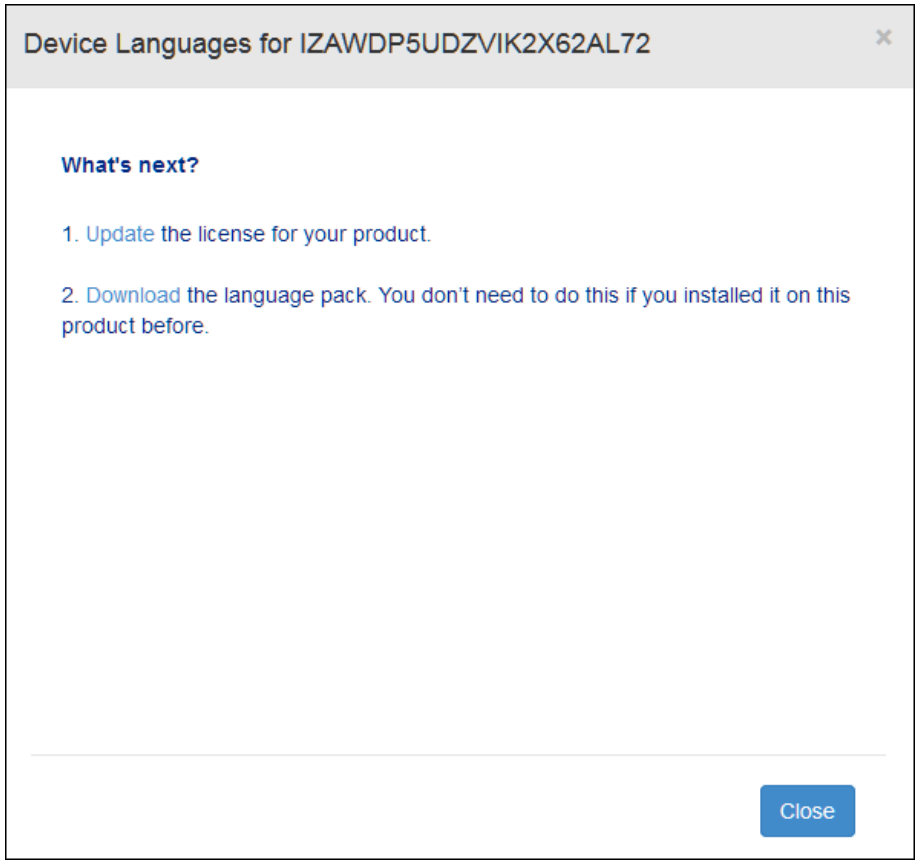
2. Select and click **Select Languages**. The following window appears.



3. Select up to five translation languages and click **Next**. The following window appears. For additional languages, click **Need more languages** and complete the form.



4. Click **Save**. The following window appears.

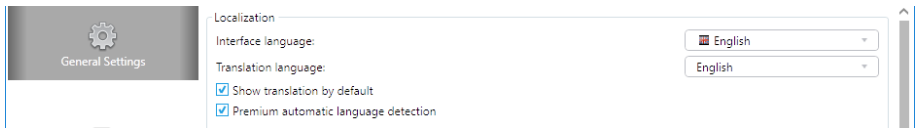


7.3. Using the feature

By default, the target language is set to the same language as the interface language. If required, you change the target language to a different language.

To choose the target language:

1. Select **Tools** > **Settings**. The following window appears.



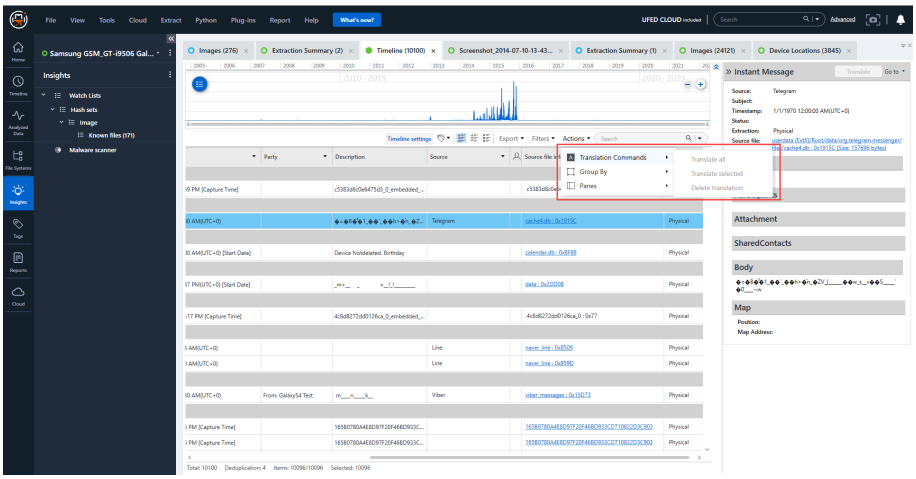
2. Select the Translation Language. That is the target language to which you want to translate the text. You can only select one Translation language. To request additional translation languages, select **Get more languages**.
3. Select the **Show translation language by default** check box to display translations by default. Clear this check box so that the translation will not appear when you translate text.

The **Smart Translator automatic language detection** check box is selected by default and automatically identifies the Smart Translator language to which you want to translate. To manually select the Smart Translator language, clear the check box in the General Settings and select the required translation language.

To translate decoded data:

1. Click to select the data that you want to translate.
2. Right-click and select **Translate selected**, or click **Actions > Translate commands** and select one of the following options:
   - **Translate all:** Translate all entries in the specified view.
   - **Translate selected:** Translate the select text only.

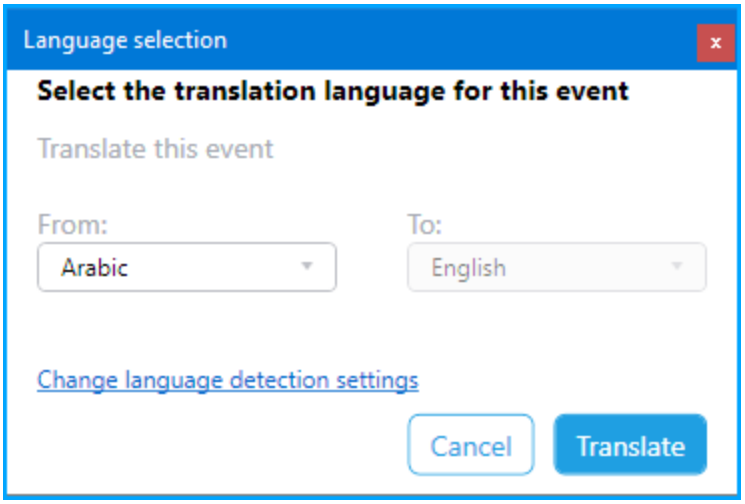
   The translated text is indicated by an orange bar.



If required, use the **Delete translation** option to delete the translated text.

To manually select the Smart Translator language:

1. Clear the **Smart Translator automatic language detection** check box under the General Settings.
2. Click the **Translate** button. The following window appears.



To view the original text:

» Right-click the text and select **View source**, or click the View source button.

To filter text:

» Click and then select one of the following options:

- » **All** to display all text.
- » **Translated** to display text that has been translated.
- » **Not translated** to display text that has not been translated.

7.3.1. Reporting

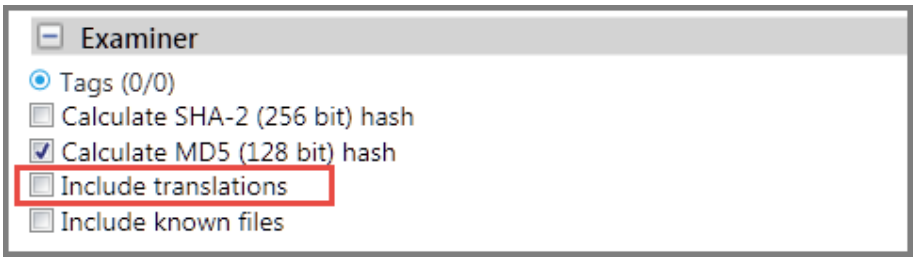
When creating reports or exporting data, you can specify whether to include the translated text or not. If you choose to display the translated text within the report, the summary table will include an additional entry called: Translated languages, with a list of the languages. The translated content appears below the original text under the heading: Translation.

To include translated text in reports, by default:

1. Go to **Tools** > **Settings** > **General Settings** > **Report Defaults**.
2. Select the **Include translation** check box.

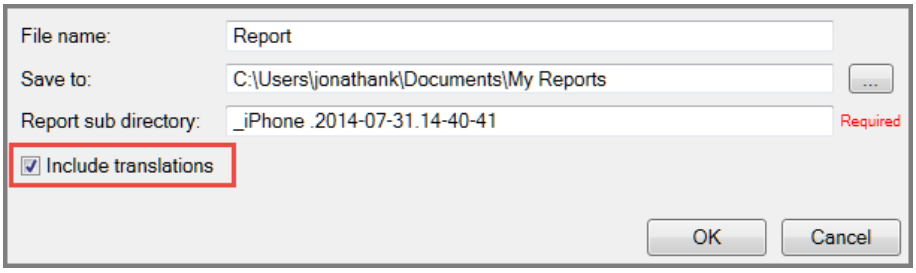
To include translations in reports:

In the report wizard, select the **Include translation** check box



To include translated text in exports:

1. Click an Export option ( ).
2. Select the **Include translation** check box.



8. Cloud extractions

Cloud extractions assists law enforcement agencies and enterprises to enhance their investigations by extracting and displaying information from cloud-based data sources such as Google Location history, iCloud backup, Facebook, Twitter, Gmail, Google Drive, Google Contacts, Google Search History, Dropbox, IMAP, Instagram, etc.

Cloud extractions reduce the time required to solve cases:

- Real-time access to an extraction of private and public user data from key cloud-based data sources, such as social media, web mail and cloud storage sources, etc.
- Normalization of forensically extracted data into a common view so users can quickly search, filter and sort data.
- Creation of customized reports for easy review and data sharing.
- Data export into other analytics tools for further investigation.

> The cloud extraction capability is only available to users that have purchased a UFED Cloud license.

UFED Cloud helps agencies leverage cloud data to solve cases faster. The key benefits of UFED Cloud include:

- **Access more than 50 applications** - Extract, preserve, and analyze cloud-based content from over 50 applications.
- **Get data faster** - Remove the dependency on service providers by using tokens or user credentials.
- **Retrieve data without need for the physical device** - Access forensically sound data that no longer resides on the physical device by retrieving cloud backups.
- **Streamline workflows** - UFED Cloud is integrated with Physical Analyzer for a seamless review process.
- **View digital activity and locations** - Get data about users' digital activity and locations from Facebook, iCloud, and Google across multiple devices.

8.1. Extracting private cloud account data

UFED Cloud supports the extraction of cloud accounts from selected apps (data sources).

The extraction wizard leads you through the five steps of the cloud extraction process:

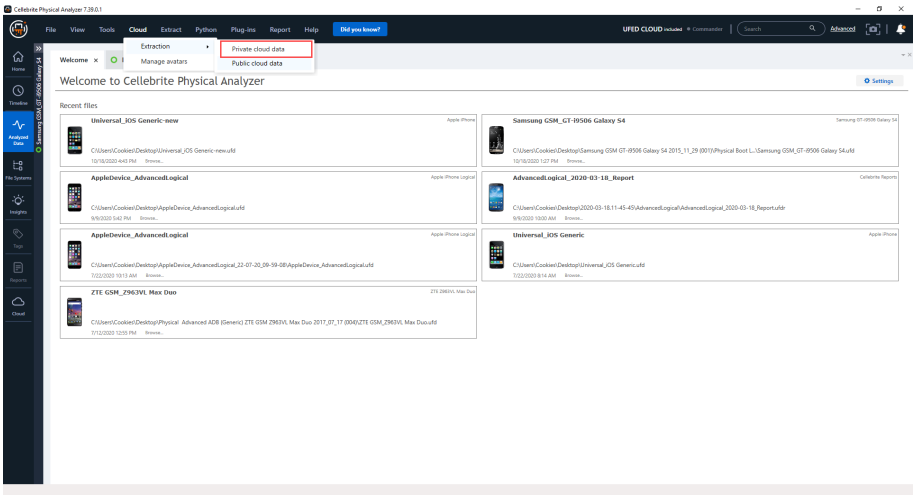
1. **Case details** - adding the case details to a new or existing case including:
   - Person details
   - Examiner details
   - Legal authorization/search warrant document upload option
   - Media classification selection

- Time zone settings
- Option to create a UFDR report automatically after extraction.
- Option to select location to save report and account package.

2. **Data sources** - selecting the data sources that are required for the extraction. It's also possible to import an account package at this stage.
3. **Validation** - validating of credentials/tokens including multi- factor authentication to access the data sources.
   - In this step it is also possible to create an account package for future use. Select data source credentials to include in the account package. The authentication state will also be saved.
4. **Extraction settings** - setting the date range, data categories, etc that are required.
5. **Summary** - summary of this cloud extraction.

Opening the cloud extraction wizard

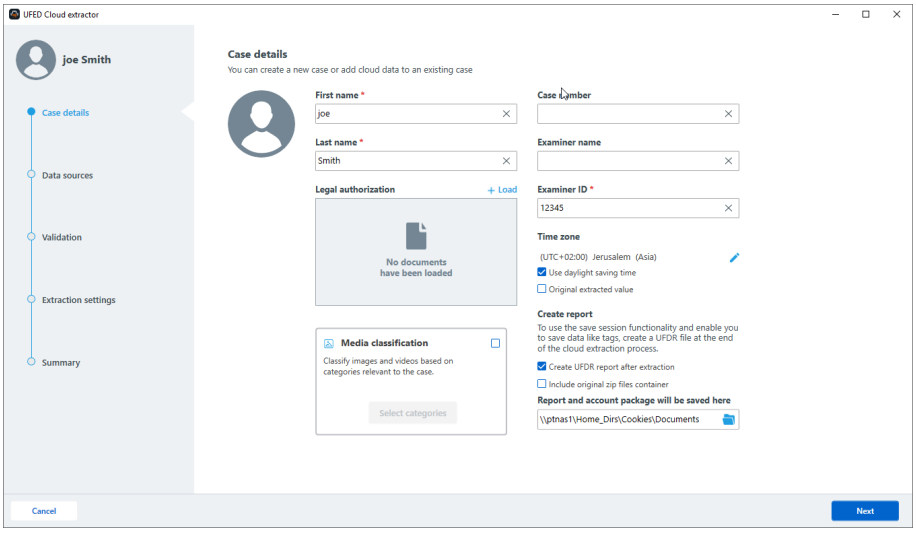
1. In the menu, click **Cloud** > **Extraction** > **Private cloud data**.



The extraction wizard appears.

8.1.1. Adding case details

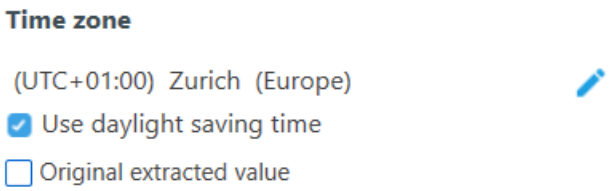
The person is the subject of the investigation and referred to as the Owner of the data.



1. In the case details screen, enter the case details including person and examiner information.

> Mandatory fields are indicated with a red border.

2. Add a picture of the person.
3. Upload legal authorization document if required.
4. Select time zone.



   a. Next to the displayed time zone, click .
   b. Select the required time zone from the drop down list.
   c. Set the time zone settings
      - **Use daylight saving time**: Select or unselect check box to enable or disable daylight saving time.
      - **Original extracted value**: Shows the time stamps as recorded in the data source.

> An extraction's time zone can be set at any point, either when creating a new person or post extraction.

5. Optionally select to run Media classification engine on the extraction. For more information on this capability, see Media classification (on page 346).

6. Select option to create UFDR report automatically after extraction.

> To use the save session functionality and enable you to save data such as tags, this option creates a UFDR file at the end of the cloud extraction process.

7. Optionally select to include original zip files container.

> If this option is selected, all files will be stored in a zip file when generating a UFDR.
>
> The zip file is saved in the same location of the UFDR. This zip file is hashed to make sure it was not tampered with. The hash (SHA1) is included in the extraction summary under the Cloud tab.

> Large files will not be included in the zip file.

8. Use default or select new path to save report and account package.
9. Click **Next** to select data sources for extraction.

8.1.2. Selecting data sources

In the Data sources screen, you can select data sources for extraction with the following methods:

- **Select data sources manually** - Select data sources from the list and enter credentials manually. Use the search bar to search for required data sources.
- **Import an account package** - A *.ucae or .ucaepc file exported from Physical Analyzer. It contains saved account tokens, cookies or user credentials which can be used to authenticate accounts in Physical Analyzer with minimal traces.

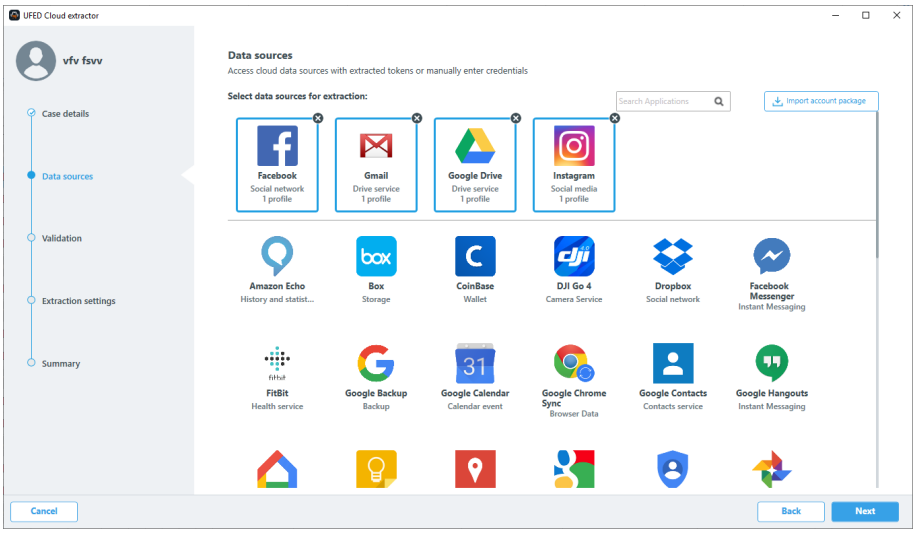
  It is also possible to import an account package that was created from a previous UFED Cloud extraction.

When using an account package, there are two methods based on where your UFED Cloud is installed:

- **UFED Cloud is installed on a separate machine:**
  - The first step is to export an account package from Physical Analyzer or from another extraction tool, such as the Cloud Login Collector.
  - The next step is to import the account package into UFED Cloud. UFED Cloud will then

display the available accounts and the user can then select which accounts to authenticate.

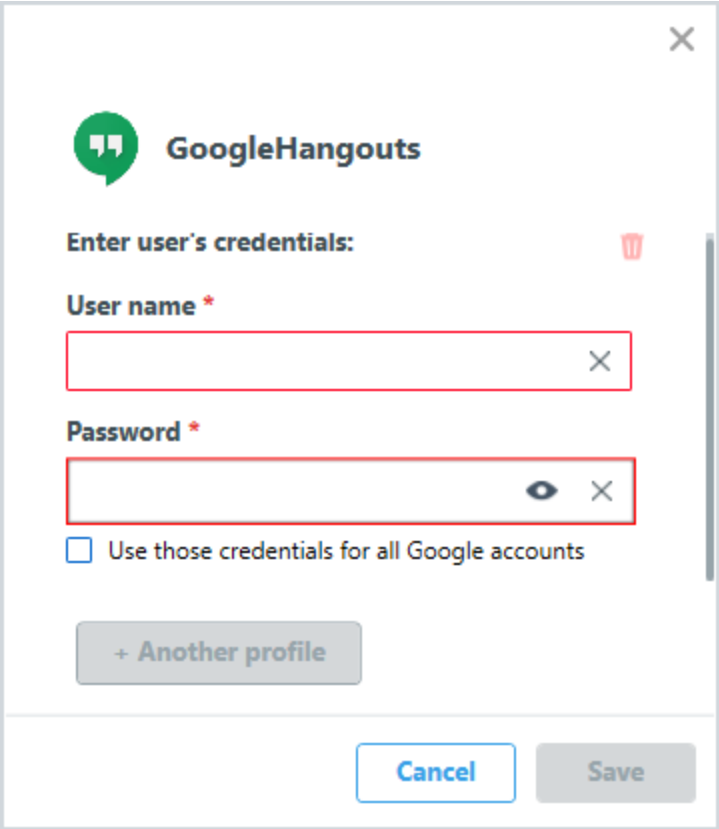
- UFED Cloud is installed on same machine as Physical Analyzer:
  - The cloud extraction is executed and displayed in Physical Analyzer without the need for an import.



Procedure

1. Select data sources for extraction:
   a. Manually select data sources.
      i. Click on the data sources that are required.
      ii. Enter credentials.
      iii. Click **+ Another profile** button to add another account related to this extraction if required.

iv. To use the same credentials for multiple apps select the check box.

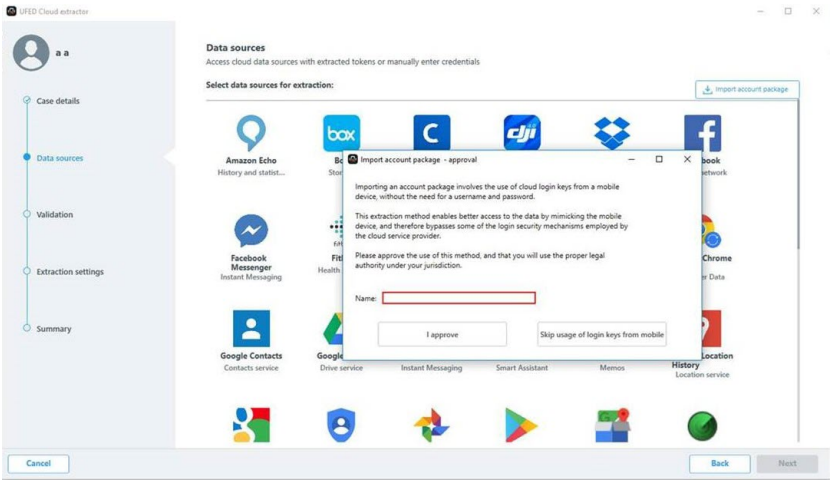


Selected data sources appear at the top of the screen. Click to unselect a data source.

b. Import an Account package.

   i. Click on the **Import account package** button.

   ii. The following window appears the first time an account package is used.



> This window provides an indication that an account package includes the use of cloud login keys from a mobile device and must include proper legal authority under your jurisdiction. Enter your full name, and click **I approve**.

   iii. Select the Account package file.

   iv. Click **Open**.

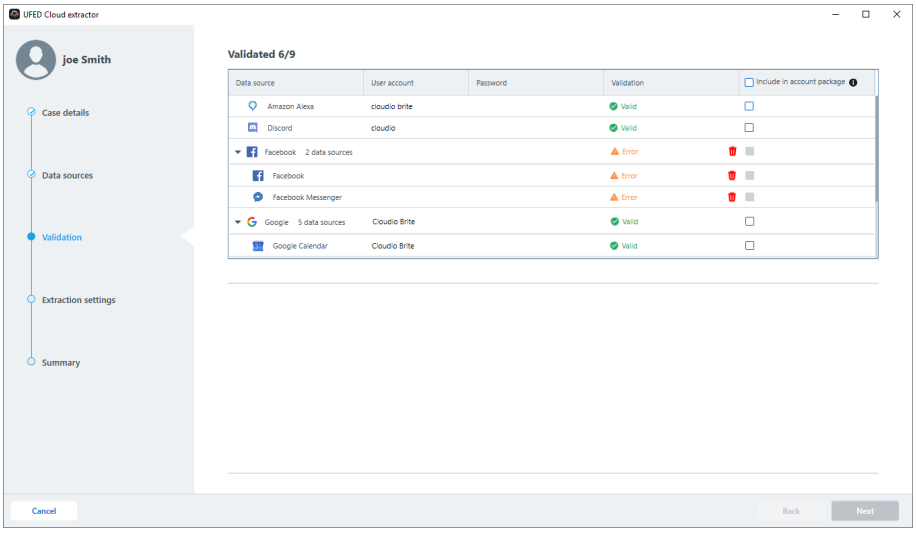
   v. The account package opens in a new tab.

   vi. Select data sources from account package.

2. Click **Next**. The validation screen appears.

8.1.3. Validating cloud account credentials/tokens

The validation screen displays a table with selected data sources, user account, password, and validation result (valid/error/QR scanning required).



Possible statuses include:

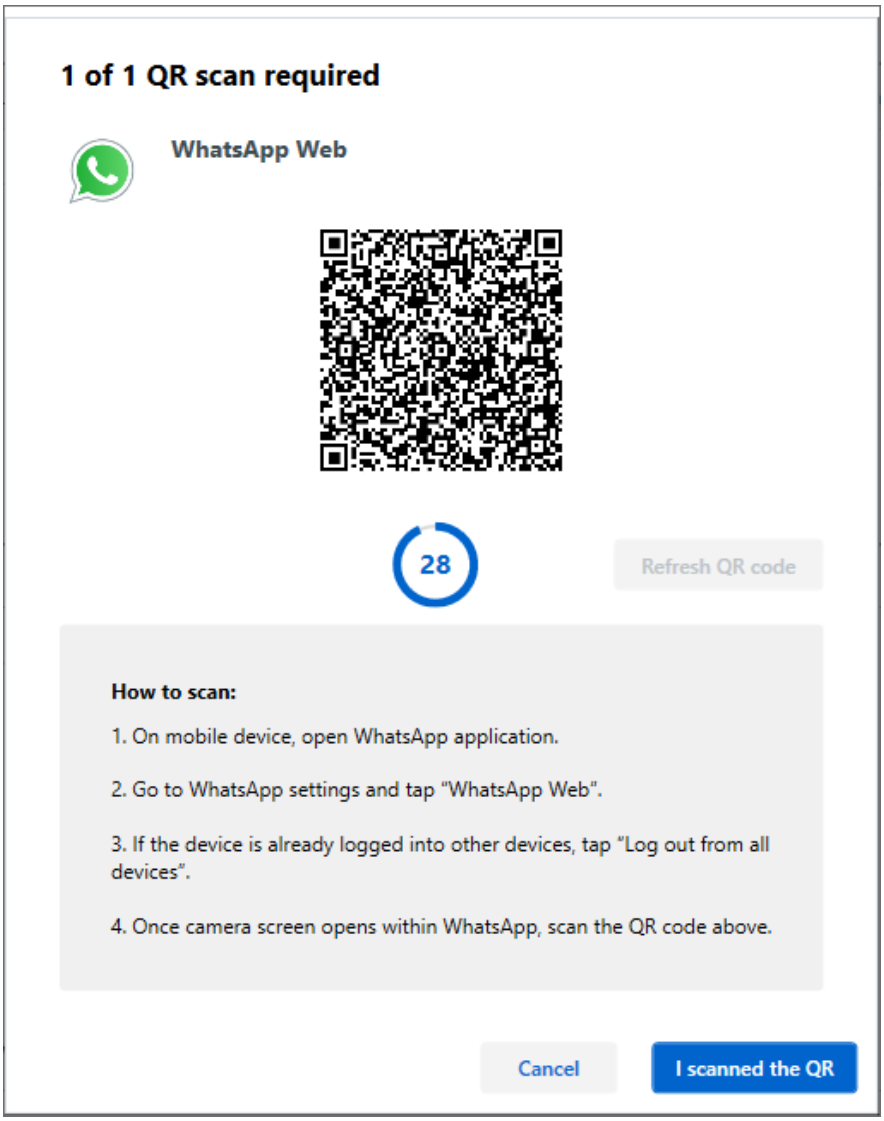
- Valid - the authentication (validation) was successful.
- Error - the authentication was unsuccessful. Hover over error to view details.
- QR scanning required - In the case the WhatsApp Web data source was selected in the previous step. For more information, see Accessing WhatsApp Web data (on page 365).

> For data sources that received an error status due to incorrect credentials, click to reenter the credentials.
>
> To delete a data source from the extraction, click .

Some sources, will require additional validation steps:

- If multi-factor authentication or CAPTCHA is required, see Multi-factor authentication and CAPTCHA (on page 220).
- If multiple Google accounts are recognized from a PC token, see Choosing from multiple Google accounts (on page 224).
- If WhatsApp Web was selected, click QR scanning required and scan the QR code to

validate.



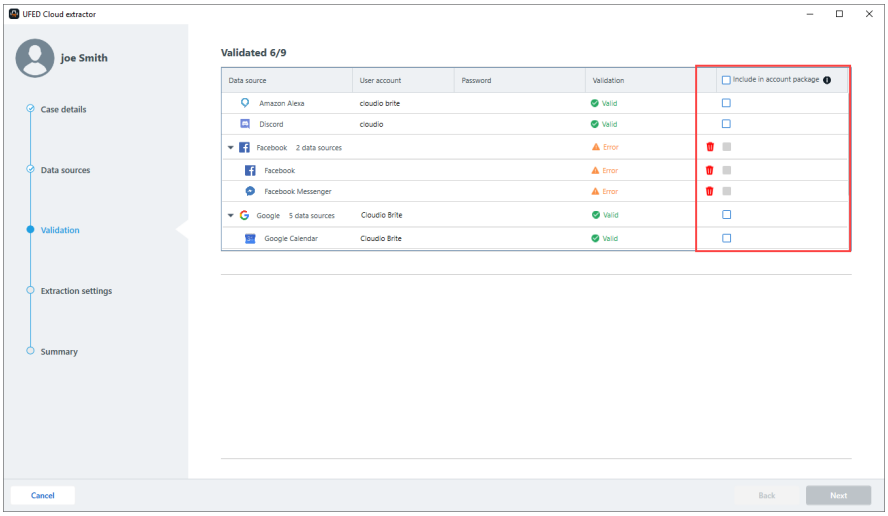
To look up a list of active accounts and their credentials, use the **Password collector.** The **Password collector** can help you overcome expired tokens or gain access to apps which are not directly supported by UFED Cloud. See Password collector (on page 223).

Notes

- Instagram uses the username instead of an email address.
- Telegram uses the phone number instead of the username.
- Google Takeout and iCloud Backup have a slightly different workflow, see their advanced options.

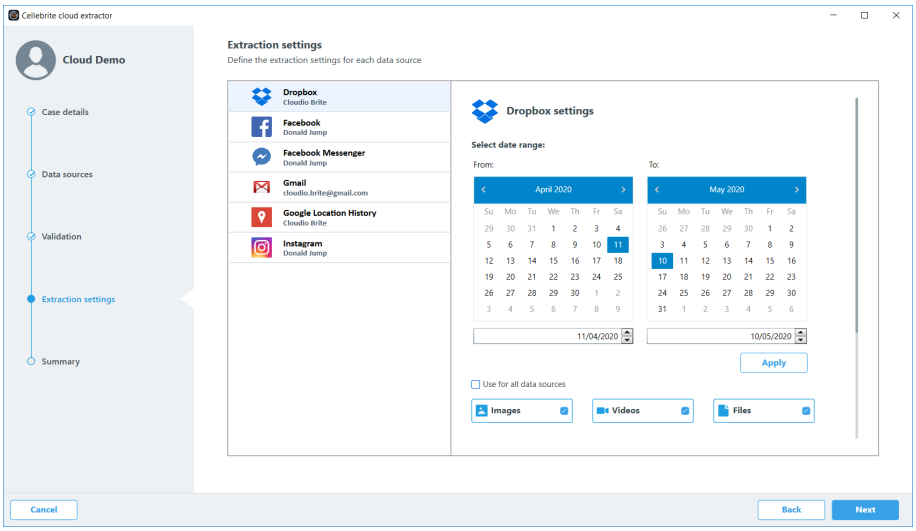
1. To create an Account package, select the data source credentials to include in the account package.

> iCloud backup, WhatsApp web, Password collector are not supported in account package creation.



2. Click **Next**. The Extraction settings screen appears.

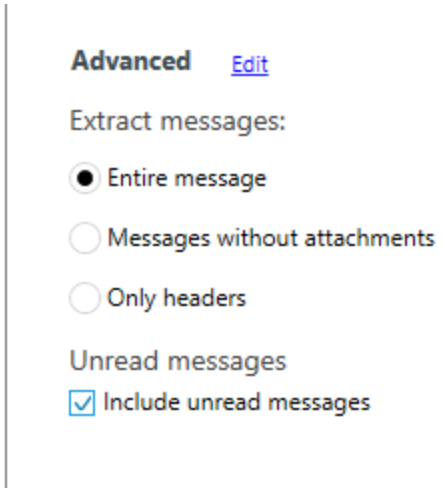
8.1.4. Managing cloud extraction settings



1. Select a date range for each data source.

> To select the same range for all data sources check **Use for all data sources.**

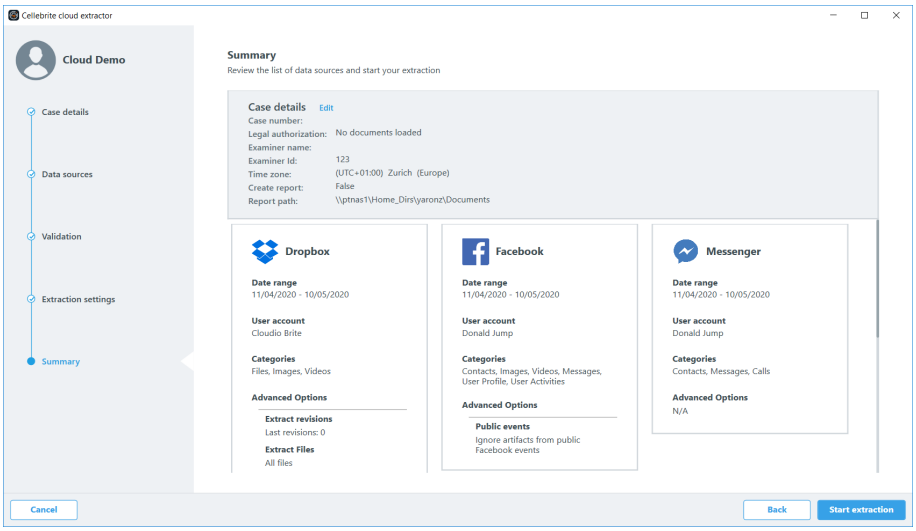
2. Select or unselect the required data categories.
3. Select the required Advanced settings. See Advanced options (on page 226).



4. Click **Next**. The Summary screen appears.

8.1.5. Viewing the summary before extraction

The summary screen displays all details and settings of the extraction.



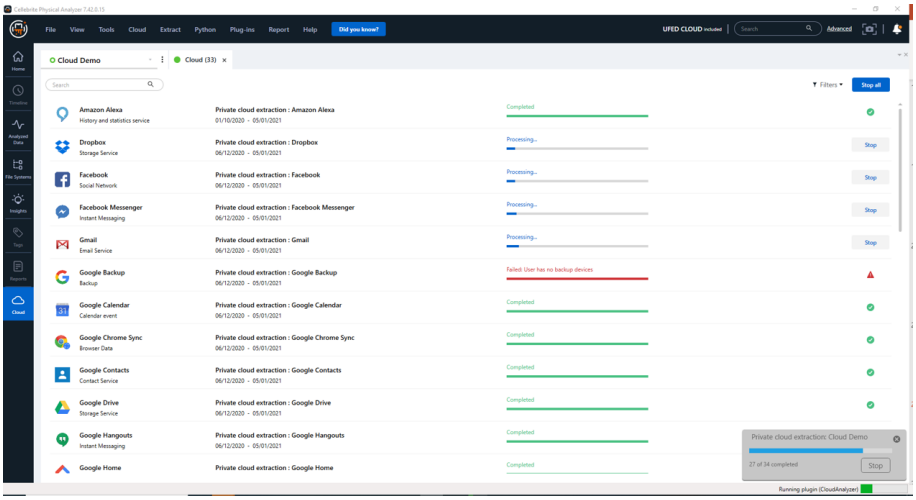
1. Click **Start extraction**.

8.1.6. Monitoring extraction progress

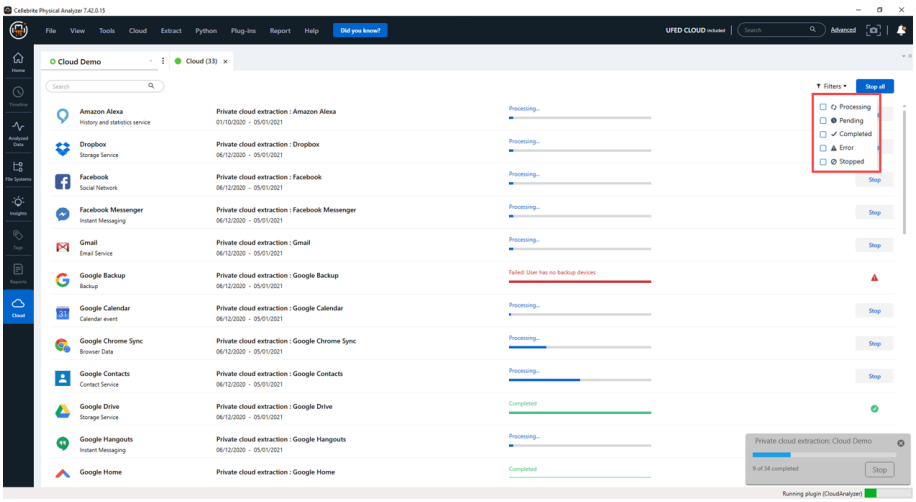
It is possible to view and track the progress and status of a cloud extraction. Using the extraction progress screen that appears as soon as the extraction starts, you can see the current status of each data source as well as the progress of the entire cloud extraction.

Possible statuses include:

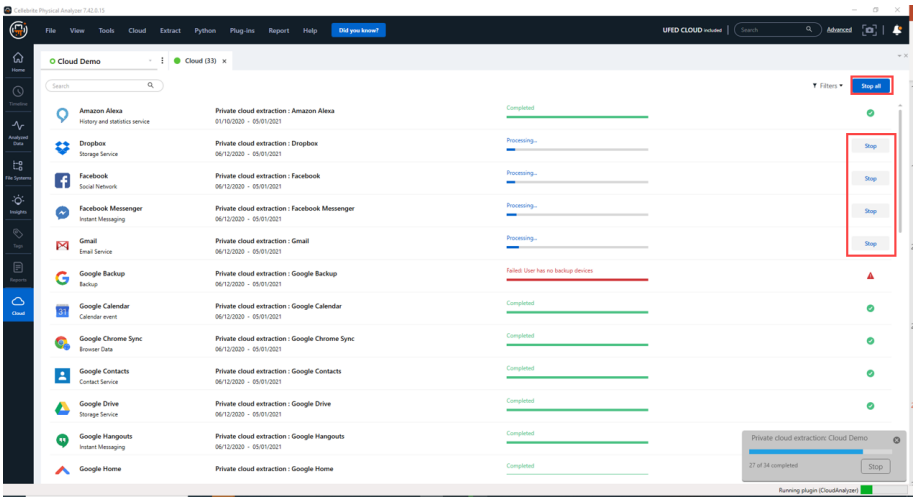
- Processing
- Pending
- Completed
- Error/failed (plus the reason for failure)
- Stopped



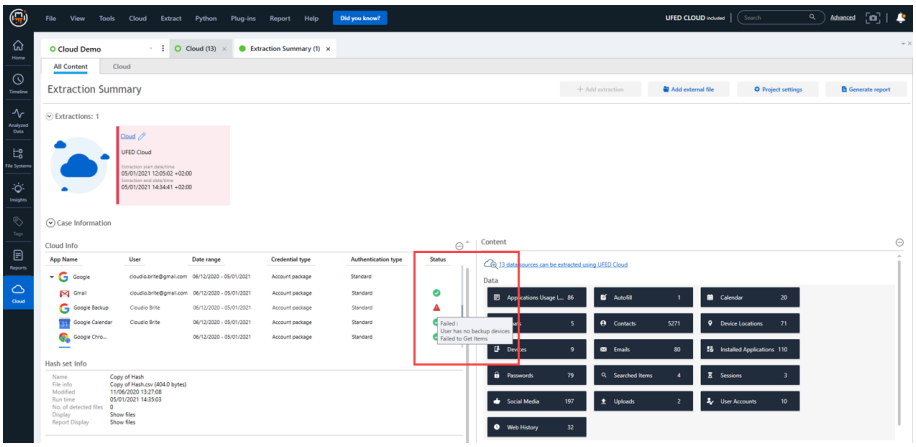
Filter the data extractions according to current status:



Cancel individual or all extractions if necessary by clicking **Stop** or **Stop all**:



Once all data sources have been extracted, the Extraction summary will display a pass/fail indication. In case of failure, the reason for the failure will be displayed:



8.1.7. Multi-factor authentication and CAPTCHA

When validating data sources, it is sometimes necessary to take extra steps to access the data. These include multi-factor authentication and CAPTCHA.

8.1.7.1. Multi-factor authentication

Multi-factor authentication refers to a temporary code sent by SMS to an account's registered number/s. Physical Analyzer supports multi-factor authentication for most data sources.

8.1.7.2. CAPTCHA

CAPTCHA refers to a challenge question designed to screen against illicit scripts.

Important notes

- Generally, this challenge is only encountered when authenticating an account using credentials.
- It can generally be avoided by using tokens from an account package.

Supported apps

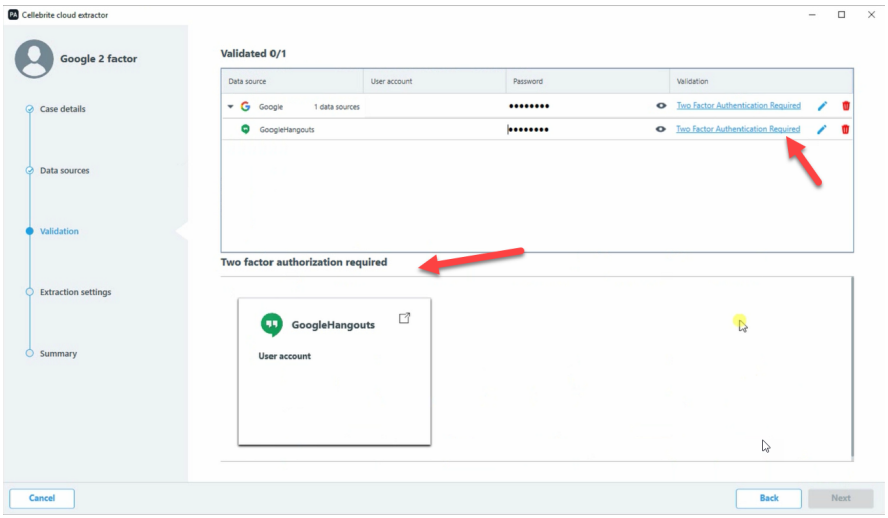
Physical Analyzer supports a CAPTCHA challenge for the following data sources:

- Amazon Shopping
- Amazon Alexa

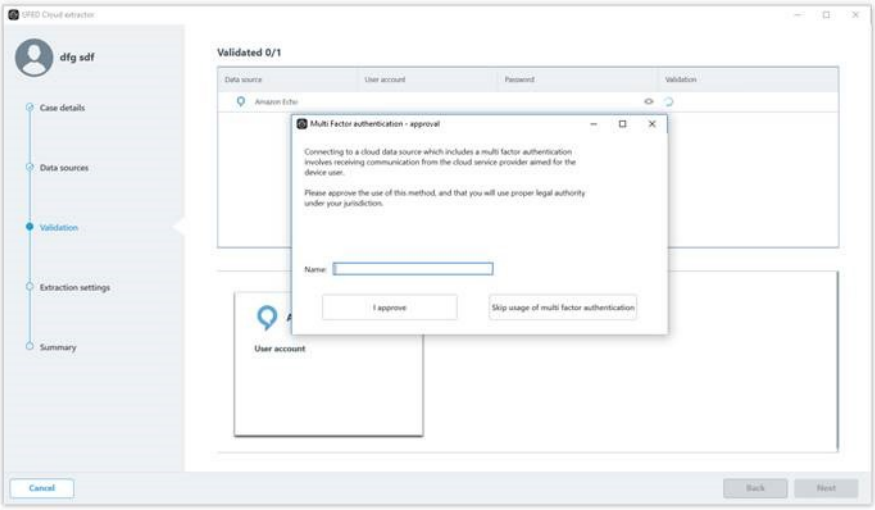
How to authenticate data sources through multi-factor authentication/CAPTCHA.

In the Validation screen of the extraction wizard, data sources that require additional authentication will be indicated.

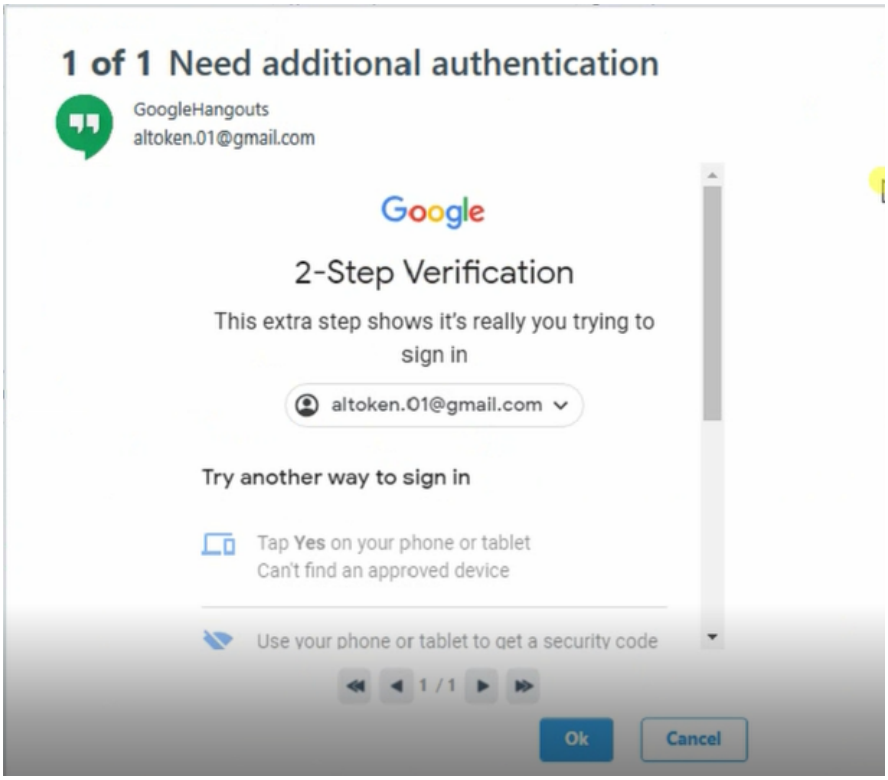
1. To begin the authentication either:
   - Click on Two Factor Authentication Required in the table row.
   - Click on the data source listed in the **Two factor authentication required** section below the validation table.



2. If this is the first time performing multi-factor authentication, the following window appears:
   a. Enter name.
   b. Click **I Approve**.



3. The authentication window appears.



4. Scroll down in the **inner** window if necessary.
5. Enter the code/CAPTCHA requirement.
6. Click **Next**.
7. If additional data sources require authentication, repeat steps 3 and 4 for each source.
8. When all sources are validated, click **Ok**.

Special cases

The flow for 2FA is mostly standard, but some apps present special circumstances or requirements.

App	Notes
iCloud	1. Authenticate a single iCloud session at a time. Otherwise, two factor authentication will encounter problems. If sent simultaneously, the authentication factors sent by different iCloud services may conflict and cancel out one another. 2. (Optional) Select to which device to send the verification code from a list of authorized devices previously defined by the account owner.
Telegram	A different sequence of steps: The app requests a phone number and then an SMS code.
Uber	A different sequence of steps: The app requests an SMS code followed by a password.

8.1.8. Password collector

When using an Account Package - regardless of its origin, whether extracted from iOS devices, Android mobile devices, Mac computers and PCs - You can look up the list of active accounts and their credentials in the **Password collector.**

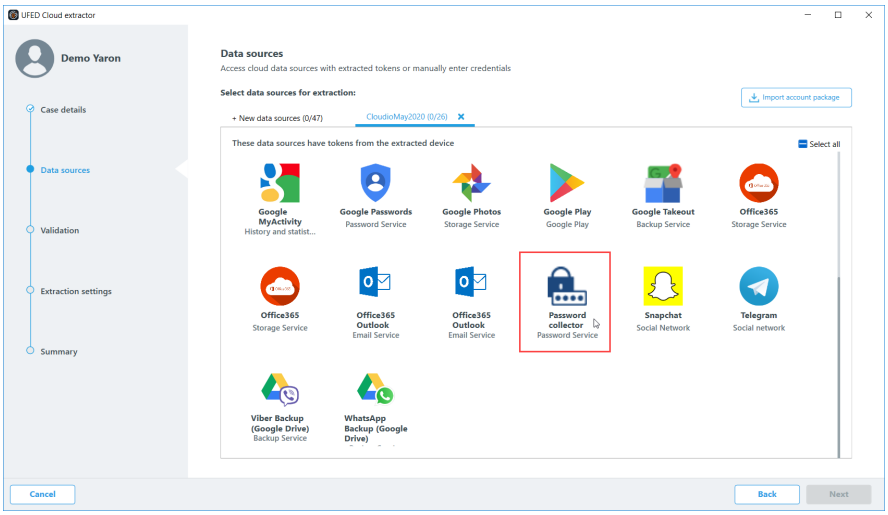
The **Password collector** can help you overcome expired tokens or gain access to apps which are not directly supported by Physical Analyzer.

To run the password collector:

1. Import an account package.

   Physical Analyzer will pull the list of apps and the account credentials extracted from the account package.

2. The list of available tokens will appear. Select the **Password collector** and proceed with the extraction.



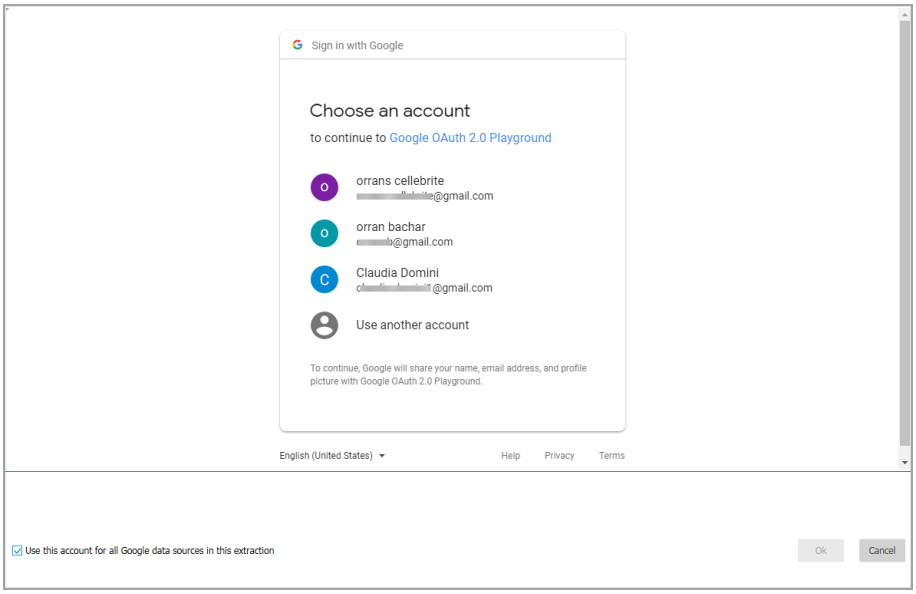
> No internet connection is required. This note pertains *exclusively* to the **Password collector**.

8.1.9. Choosing from multiple Google accounts

When multiple Google account credentials are saved in a PC token and imported to UFED Cloud in an account package, you will need to choose which account to validate and extract.

To choose a Google account:

1. Select the relevant Google data source and click **Next**. The following window appears.



2. Click **Choose a Google account**. The following window appears.

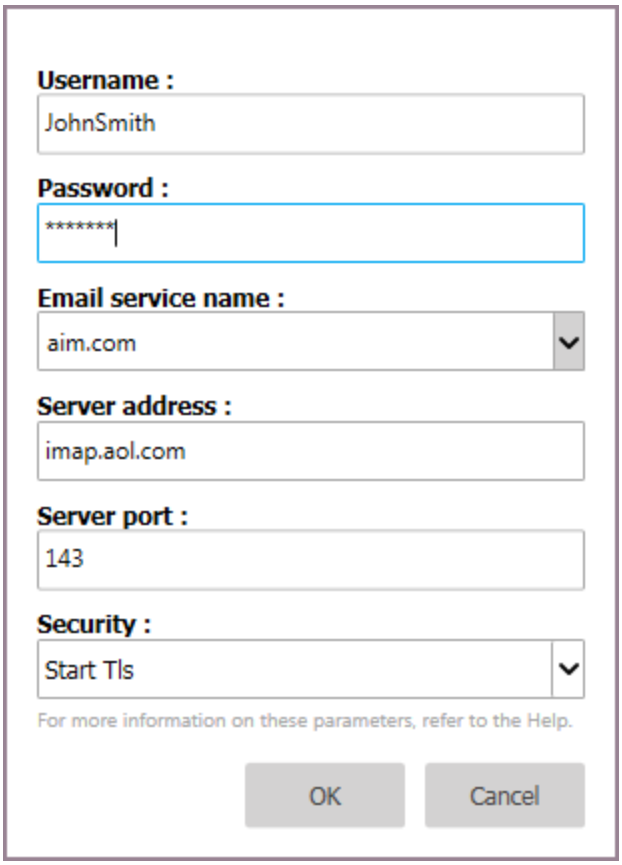
3. Choose the desired account and click **Ok**.

> If you've selected multiple Google data sources for extraction, you may select to use one account for all Google data sources in the extraction.

> If you've selected a Google account with two-factor authentication that is currently logged out, it will trigger the two-factor authentication process.

8.1.10. IMAP parameters

When adding an IMAP data source, the Server address, Server port and Security options are displayed for popular accounts. You can add additional accounts by entering information in the Email service name box and completing the other fields. You can also remove accounts that are not required. If you would like to add an account that does not appear in the list, search the Internet for the required IMAP information. An IMAP example for an AIM account is displayed next.



IMAP parameters:

- **User name:** Login information for IMAP and SMTP, login name (account name). This is usually the same as the email address. e.g., JohnSmith@aim.com.
- **Password:** Password to access the email account.
- **Email service name:** Name of the email account. e.g., aim.com.
- **Server address:** Incoming mail server for IMAP. e.g., Aim uses imap.aol.com.
- **Server port:** TCP port for IMAP communication. e.g., the default Aim IMAP port is 143.
- **Security:** Secure connection for IMAP server. e.g., Aim uses StartTls. The options are:
  - SslOnConnect: The connection should use SSL or TLS encryption immediately.
  - StartTls: Elevates the connection to use TLS encryption immediately after reading the greeting and capabilities of the server.
  - StartTlsWhenAvailable: Elevates the connection to use TLS encryption immediately after reading the greeting and capabilities of the server, but only if the server supports the STARTTLS extension. If you are not sure which security option to use, select the SslOnConnect option, which is used by most services.

8.1.11. Advanced options

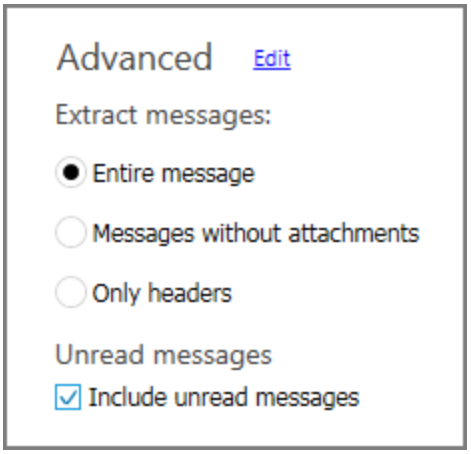
Advanced options help you narrow down the extraction parameters. For example, you can select a specific timeframe, a specific backup file, or a specific account from several linked accounts.

In this section:

8.1.11.1. Advanced options for email services

To specify optional advanced settings for email services such as Gmail and IMAP:

1. In the Extractions settings window, select a data source and scroll down.
2. Next to Advanced, click **Edit** . The advanced options appear in the window.



- **Extract messages:** The amount of content to extract from an email message.
  - **Entire message:** Extract all parts of the email message. This is the default option.
  - **Message without attachments:** Extract the email message (header and email body) without any attachments.
  - **Only headers:** Extract only the message headers (e.g., To, From, Date, Subject). This option is *not* available when using an account package[1] from an Android device.
- **Include unread messages:** Clear this check box if you do not want to include unread messages in the extraction. This can be useful if the legal authority does not cover messages that have not yet bean read by the suspect.

8.1.11.2. Advanced options for Google Takeout

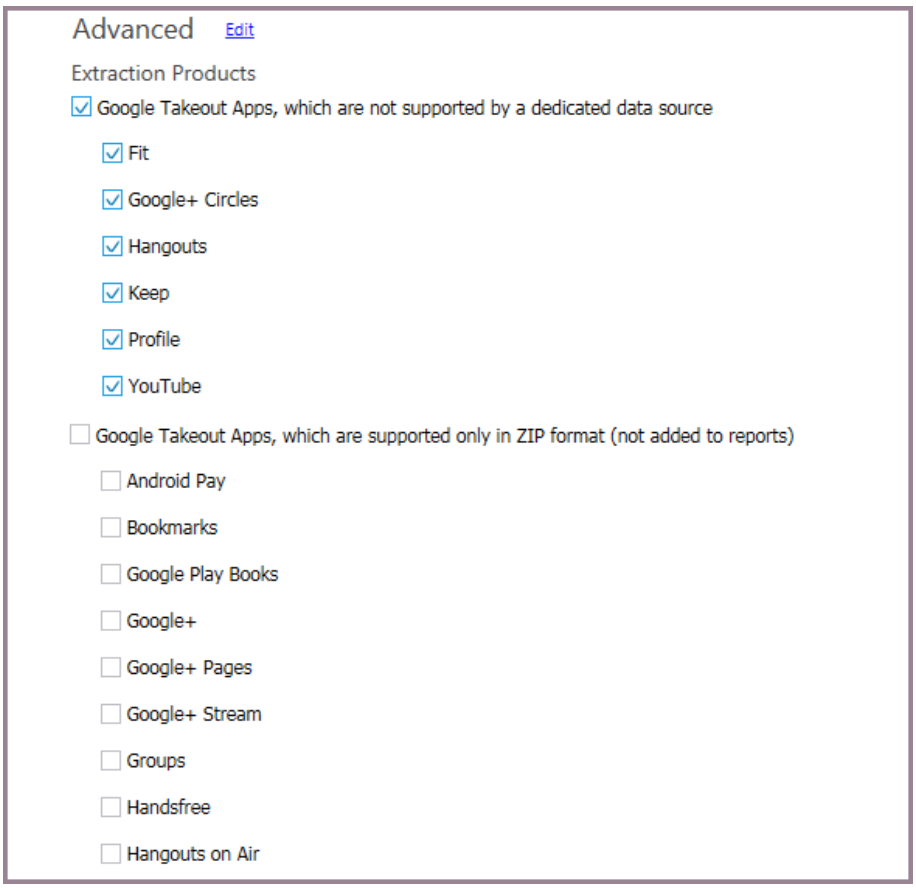
Extract a subject's devices content backup stored across Google apps. The advanced options allow you to choose which Google app data to display.

> The date range option is not relevant for Google Takeout extractions.

[1]An export file in .ucae format that contains user credentials, tokens or cookies, that can be imported and used to authenticate cloud accounts. An account package can be exported from Physical Analyzer, Cloud Login Collector and more.

To specify advanced settings for Google Takeout:

1. In the Extractions settings window, select Google Takeout and scroll down.
2. Next to Advanced, click **Edit**. The advanced options appear.



There are 2 types of Google apps available for extraction:

- Apps that are only supported via Google Takeout (these apps are selected by default)
- Apps that are only supported in ZIP format

> To reduce extraction time and increase effectiveness, access, Google apps with dedicated data sources should be extracted using the dedicated data source (e.g., Chrome, Drive, Photos, Mail, etc.)

3. Select the required data sources and click **Start extraction**. We highly recommend selecting only the apps you need for your case, to minimize extraction time.

Space limitation: Google Drive storage affects the success of Google Takeout extractions

Google Takeout uses the available storage in the person's Google Drive account to transfer the data into UFED Cloud. The default Google Drive size is 15GB, and the amount of space

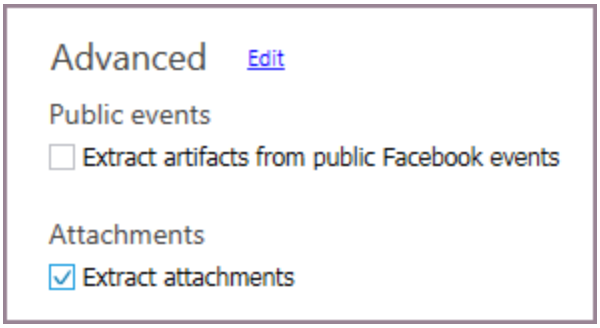
required can vary widely based on the amount of data collected. We therefore recommend focusing on the apps that will provide the most value to your investigation.

The Takeout archive will remain saved in the person's Google Drive account. If the person's Google Drive is close to full, extraction options via Google Takeout in UFED Cloud are very limited, and may fail. In this case, the data can be downloaded manually as a ZIP file and imported manually into Physical Analyzer.

8.1.11.3. Advanced options for Facebook

To specify optional advanced settings for Facebook:

1. In the Extractions settings window, select a data source and scroll down.
2. Next to Advanced, click **Edit** . The advanced options appear in the window.



- **Extract artifacts from public Facebook events:** Extract all Facebook events including public events. This option is cleared by default.
- **Extract attachments:** Extract all parts of the message. This is the default option. To download messages (header and email body) without attachments, clear this option.

8.1.11.4. Advanced options for statistics services

To specify optional advanced settings for statistic services such as Google Search History:

1. In the Extractions settings window, select a data source and scroll down.
2. Next to Advanced, click **Edit** . The advanced options appear in the window.

» **All searches:** Extract the search history for all searches including text, voice and visited pages. This is the default option.

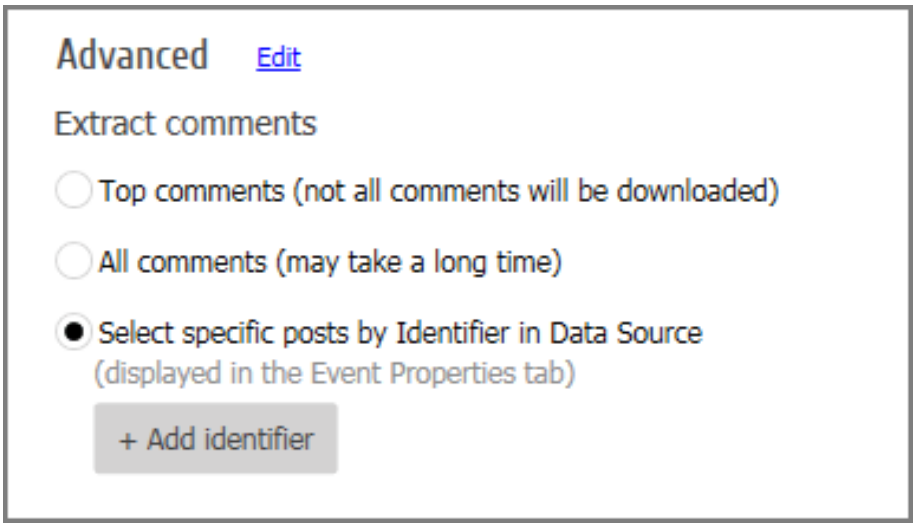
» **Specific text:** Extract the search history for a particular search word or phrase including text, voice and visited pages. This is a simple text search with spaces between words.

> Google stores the list of mobile devices that were used to access the Google account.

8.1.11.5. Advanced options for social media

To specify optional advanced settings for social media such as Instagram:

1. In the Extractions settings window, select a data source and scroll down.
2. Next to Advanced, click **Edit**. The advanced options appear in the window.



» **Top comments:** Download top comments only. This does not download all the comments.

» **All comments:** Download all comments - may take a long time to complete, depending on the number of comments.

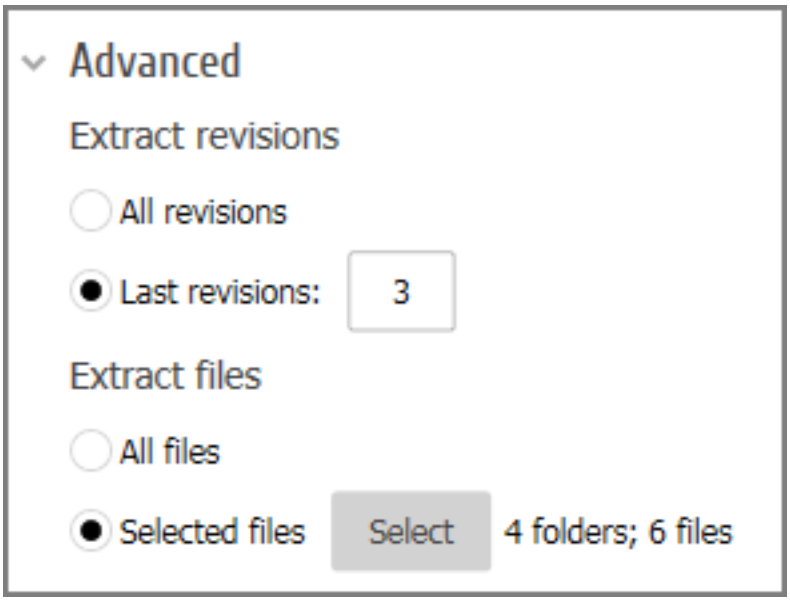
» **Select specific posts by Identifier in Data Source:** Select the post to be downloaded by the Identifier in the Data Source[1]. The identifier in the data source can be determined from a previous extraction and is displayed in the Event Properties tab. Click **Add identifier** to add additional identifiers.

[1]The source of the extracted data (e.g., Facebook, Google Takeout, Dropbox).

8.1.11.6. Advanced options for storage services

To specify optional advanced settings for storage services such as Dropbox and Google Drive:

1. In the Extractions settings window, select a data source and scroll down.
2. Next to Advanced, click **Edit** . The advanced options appear in the window:

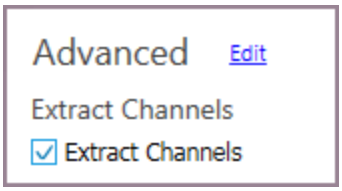


- **Extract revisions:** The number of revisions to extract per file from Dropbox and Google Drive.
  - **All revisions:** Extract all revisions of images, videos and files.
  - **Last revisions:** Specify the number of revisions to extract for images, videos and files. The default is 0, which means no revisions are extracted.
- **Extract files:** Specify folders and files to be extracted from Dropbox and Google Drive.
  - **All files:** Extract all the data. This is the default option.
  - **Selected files:** Specify the data (folders and files) that you would like to extract.

8.1.11.7. Advanced options for Telegram

To specify optional advanced settings for Telegram:

1. In the Extractions settings window, select a data source and scroll down.
2. Next to Advanced, click **Edit** . The advanced options appear in the window.



- **Extract channels:** Channels are a tool to broadcasting public messages to large audiences and can have an unlimited number of members.

8.1.12. Cloud Login Collector

The Cloud Login Collector is a dedicated Windows tool to export access cookies from a Windows computer. The tool produces an account package that contains Google, Facebook, Facebook Messenger, Instagram, LinkedIn, and Twitter browser tokens, as well as iCloud, OneDrive and Telegram access tokens. You can select where the account package is saved. At the end of the process, you will receive a list of accounts from which the login information was exported.

To export an account package:

1. Go to **MyCellebrite** > **Downloads** and copy the PC Collector .exe file to a USB mass storage device.
2. Insert the USB mass storage device into a USB port on the relevant PC.
3. Browse to and double-click the .exe file.
4. An account package is created as a **.ucaecp file** in the same folder where the .exe file is saved. A log file is also created.

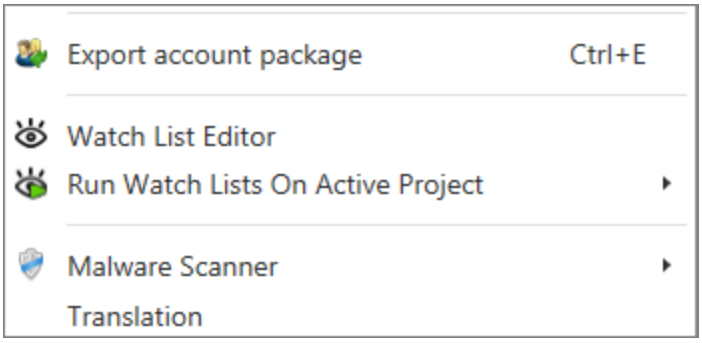
8.1.13. Exporting an account package from Physical Analyzer

Export an account package to extract cloud accounts using tokens.

> This step is only necessary if UFED Cloud is installed a separate machine than Physical Analyzer.

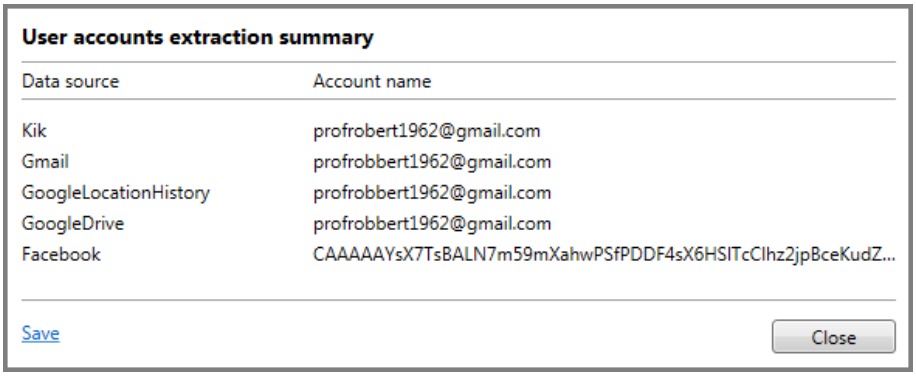
To export an account package:

1. Open an extraction in Physical Analyzer.
2. Select **Tools** > **Export account package**.



   The Save As window appears.

3. Click **Save** to save the Export file (*.ucae) file. The following window appears.



User accounts extraction summary

Data source	Account name
Kik	profrobert1962@gmail.com
Gmail	profrobbert1962@gmail.com
GoogleLocationHistory	profrobbert1962@gmail.com
GoogleDrive	profrobbert1962@gmail.com
Facebook	CAAAAAYsX7TsBALN7m59mXahwPSfPDDF4sX6HSITcClhz2jpBceKudZ...

Save Close

4. Click **Save** to save a text file summary of the extracted user accounts, or click **Close** to complete the process. (The summary may be useful when preparing search warrants, or to share with other investigators.)

> Multiple entries for the same data source may relate to different accounts that were used on the device, or to previous login information for the same account.

8.2. Extracting public cloud account data

View the public activity of a social media profile anonymously. To do this, you will use an avatar[1], that is a Facebook, Instagram, or Twitter "fake" account specifically created for this purpose.

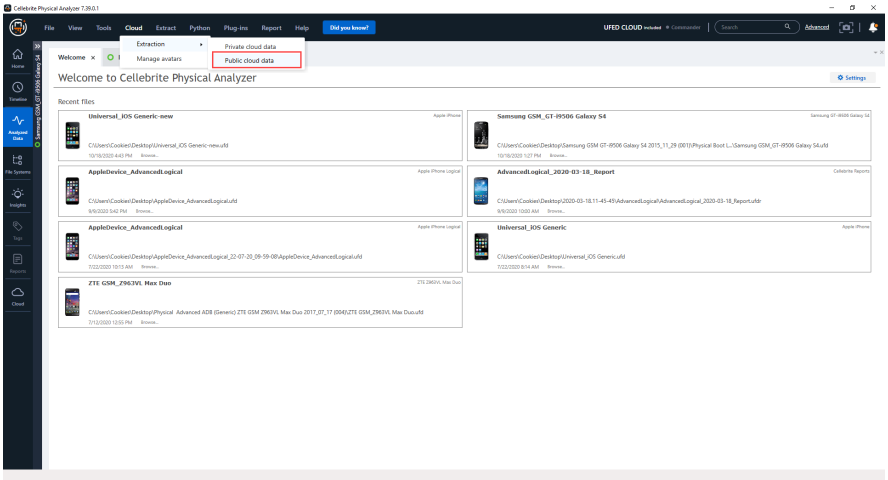
The avatar profile should never be a "real" profile as it is at risk of being blocked by the service provider for suspicious activity.

UFED Cloud will extract activity that is visible to the avatar. Therefore the data available for extraction is dependent on the relationship between the profiles. For example, a friend of a friend may be able to extract more data than a stranger.

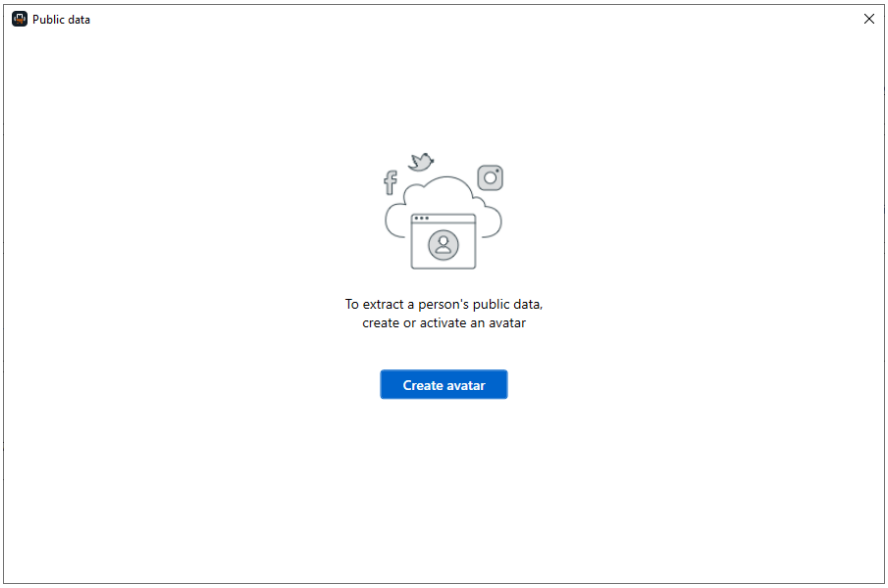
[1] A social media profile that you can use to extract public data. Note: Avatars are public profiles, and as such, are exposed to public review.

To extract a public data source:

1. In the menu, click **Cloud** > **Extraction** > **Public cloud data**.

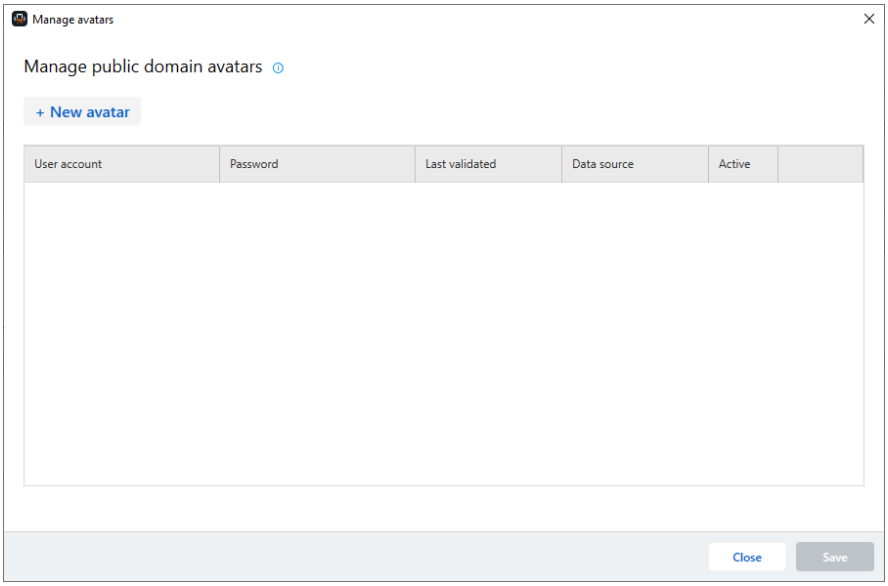


2. If you haven't created an avatar, the following screen appears:

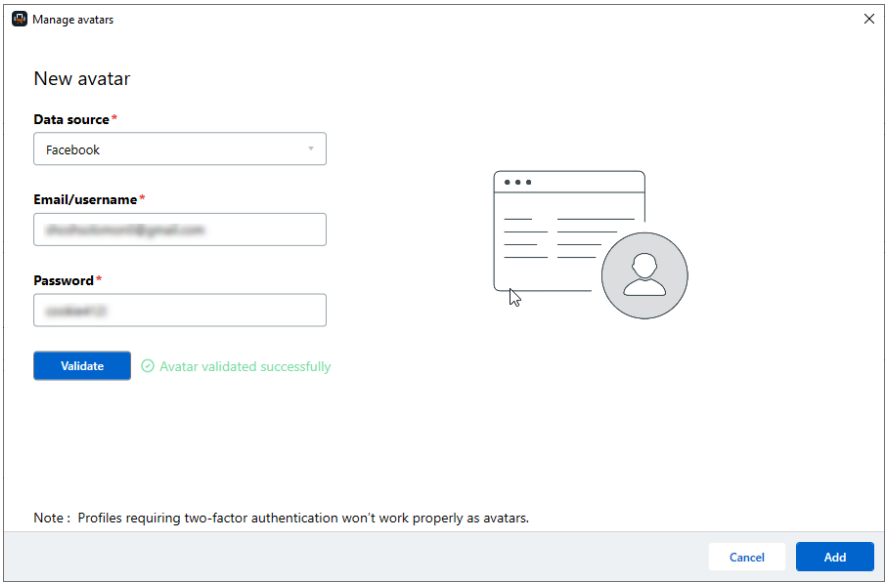


> If you have already created at least one avatar, you can skip this step.

3. Click **Create avatar**.
4. Click **New avatar.**



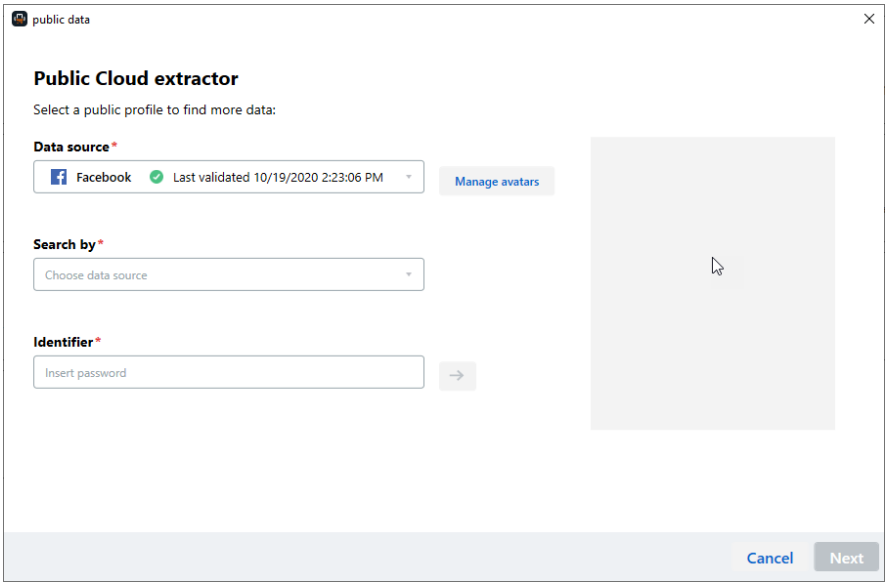
5. Select the avatar account data source.
6. Enter the Email/username of avatar account.
7. Enter password.
8. Click **Validate**.
9. Once validated, click **Add**.



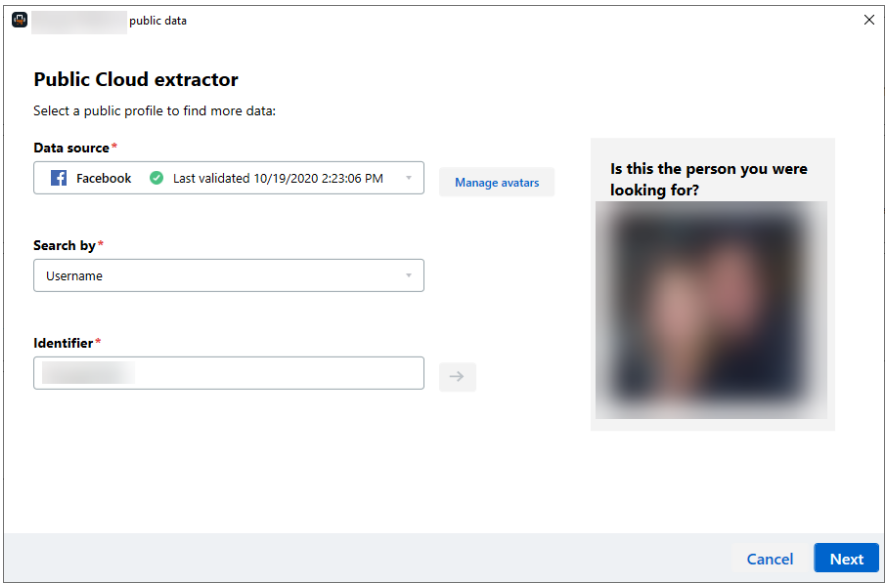
10. In the Public Cloud extractor window, select the data source.
11. Select the search by option (User ID, Username, Phone, or Email).

> Usernames and User IDs are part of a person's public profile. A Username is the web address to a person's profile or page, for example 'facebook.com/username'. A User ID is a string of numbers that is connected to a data source profile.

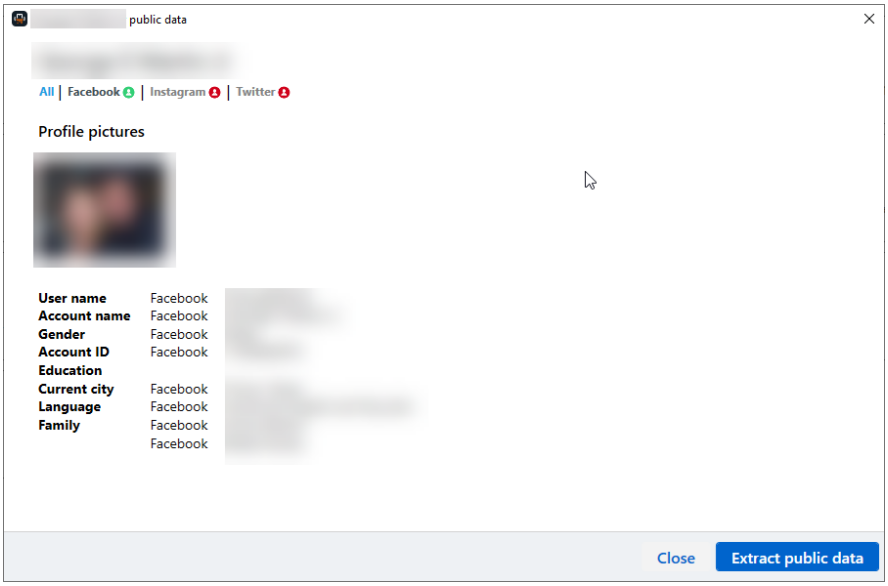
12. Enter the identifier for the Search by option.
13. Click the arrow button.



14. The system will suggest a person.
15. Click **Next**.



16. A summary of the person's public data appears.
17. Click **Extract public data** to execute the extraction.



For further information on creating and managing avatars, see Creating a public domain avatar (on page 305).

8.3. Supported content

Following is a list of data sources (and apps) supported by UFED Cloud and the types of content that can be extracted for each. About content categories

Data source	Messages	Images	Videos	Files	Contacts	Calls	Locations	User profile	User activity	Back ups
Android Backup[1]	√[2]									
Amazon Alexa	√	–	–	–	√	–	–	√	√	–
Box	–	√	√	√	–	–	–	–	√	–
Coinbase	–	–	–	–	–	–	–	√	√	
Discord	√	√	√	√	√	√	–	√	–	–
DJI Go 4	–	√	√	–	√	–	–	√	√	–
Dropbox	–	√	√	√	–	–	–	–	–	–
Facebook	√	√	√	–	√	–	–	√	√	–
Facebook Messenger	√	–	–	–	√	–	–	–	–	–
Fitbit	√	–	–	–	√	–	–	√	√	–
Generic email (IMAP)	√	–	–	–	–	–	–	–	–	–
Gmail	√	–	–	–	–	–	–	–	–	–
Google Backup	√	–	–	–	–	√	–	√	√	–
Google Calendar	–	–	–	–	–	–	–	–	√	–
Google Chrome Sync	–	–	–	–	–	–	–	√	√	–

[1]This data source is only available if you have Virtual analyzer installed on the same machine.

[2]This includes nearly all data and settings stored on the device i.e., text messages, call logs, application information, and device settings.

Data source	Messages	Images	Videos	Files	Contacts	Calls	Locations	User profile	User activity	Back ups
Google Contacts	–	–	–	–	√	–	–	–	–	–
Google Drive	–	√	√	√	–	–	–	–	–	–
Google Hangouts	√	–	–	–	√	√	–	–	–	–
Google Home	–	–	–	–	–	–	–	–	√	–
Google Keep	–	–	–	–	–	–	–	–	√	–
Google Location History	–	–	–	–	–	–	√	–	–	–
Google My Activity	–	–	–	–	–	–	–	√	√	–
Google Passwords	–	–	–	–	–	–	–	√	–	–
Google Play	–	–	–	–	–	–	–	√	–	–
Google Photos	–	√	√	–	–	–	–	–	√	–
Google Takeout	√									
Google Tasks	–	–	–	–	–	–	–	–	√	–
iCloud Backup	√[1]									
iCloud (Real-Time Location)	–	–	–	–	–	–	√	√	–	–
iCloud Data	–	√	√	–	√	–	–	–	√	–
iCloud Drive	–	√	√	√	–	–	–	–	–	–
Instagram	√[2]	–	–	–	√	–	–	–	–	–

[1]This includes nearly all data and settings stored on the device i.e., text messages, call logs, application information, and device settings.

[2]Images/videos

Data source	Messages	Images	Videos	Files	Contacts	Calls	Locations	User profile	User activity	Back ups
iTunes Purchases	–	–	–	–	–	–	–	–	√	–
Line (Google/iCloud)	√	√[1]	√[2]		√			√		
LinkedIn	√	–	–	–	√	–	–	√	–	–
Lyft	–	–	–	–	–	–	–	√	√	–
Magenta Cloud	–	√	√	√	√	–	–	√	√	–
Microsoft Office 365	–	√	√	√		–	–	√	–	–
Microsoft Outlook 365	√	–	–	–	√	–	–	√	√	–
OkCupid	√	–	–	–	√	–	–	√	–	–
One Drive	–	√	√	√	–	–	–	–	–	–
Password collector	–	–	–	–	–	–	–	√	–	–
Samsung Backup	√	–	–	√	√	√	–	√	–	–
Skype	√	–	–	–	√	√	–	√	–	–
Slack	√	–	–	–	√	√	–	√	√	–
Snapchat	√	√	√	–	√	-	–	√	-	–
Telegram	√	–	–	–	√	–	–	–	–	–
TikTok	√	√	√		√			√		
Twitter	√	–	–	–	√	–	–	–	–	–
Uber	–	–	–	–	–	–	–	√	√	–

[1] iOS only.

[2] iOS only.

Data source	Messages	Images	Videos	Files	Contacts	Calls	Locations	User profile	User activity	Back ups
Viber	√	–	–	–	–	–	–	–	–	–
VK	√	√	√	√	√	–	–	√	–	–
WhatsApp Web	√	√	√	√	√					
WhatsApp Backup (credentials)[1]	√	√	√	√	√	√	–	–	–	–

[1]When authenticating WhatsApp backup from iCloud using only credentials, only attachments are extracted. Text messages will not be extracted. In order to get messages, contacts, and calls, you will need to upload an account package from a device that had the same WhatsApp account installed. For WhatsApp backup from Google Drive, no account package is needed for the extraction. The authentication process will disconnect active WhatsApp session on the device.

8.3.1. Supported apps by extraction method

Data Source	iOS Full File System (Premium)	iOS Advanced Logical Full File System (Using UFED4PC)	Android Physical Extraction	PC token	Username & Password
Amazon Alexa/Echo	√	√	√		√
Android backup			√		√
Box		√	√		√
CoinBase	√		√		√
Discord	√	√	√		√
DJI GO 4	√	√	√		√
Dropbox			√		√
Facebook	√	√	√	√	√
Facebook Messenger		√	√		√
FitBit	√	√	√		√
Gmail	√	√	√		√
Google Calendar	√	√	√		√
Google Chrome Sync	√	√	√		√
Google Contact	√	√	√		√
Google Drive	√	√	√		√
Google Hangouts	√	√	√		√
Google Home	√	√	√		√
Google Keep	√	√	√		√
Google location history	√	√	√		√

Data Source	iOS Full File System (Premium)	iOS Advanced Logical Full File System (Using UFED4PC)	Android Physical Extraction	PC token	Username & Password
Google MyActivity	√	√	√		√
Google Photos	√	√	√		√
Google Play	√	√	√		√
Google Takeout	√	√	√		√
iCloud Backup					√
iCloud Web					√
Instagram	√		√	√	√
Line (Google/iCloud)	√	√	√		√
LinkedIn	√	√	√	√	√
Lyft	√	√	√		√
Magenta			√		√
Office365			√		√
Office Outlook			√		√
OkCupid	√		√		√
OneDrive	√	√	√	√	√
Samsung Backup					√
Skype	√	√			√
Slack	√	√	√		√
Snapchat			√		
Telegram			√		√
TikTok	√	√	√		√
Twitter	√	√	√		√

Data Source	iOS Full File System (Premium)	iOS Advanced Logical Full File System (Using UFED4PC)	Android Physical Extraction	PC token	Username & Password
Uber			√		√
Vkontakte	√	√	√		√
WhatsApp Web					√
iCloud WhatsApp backup					√
Google WhatsApp Backup	√		√		√

8.3.2. Cloud Login Collector: Supported tokens & OS

When using the Cloud Login Collector to extract an account package, the data available for extraction depends on the computer's operating system and browsers.

The table below lists which apps and desktop apps are supported and under what conditions. See also SupportedExtractionMethods.htm.

Operating system	Supported browsers	Supported desktop apps	Supported data sources
Windows 7	Chrome Internet Explorer Firefox	iCloud Backup OneDrive[1] Skype[2]	box Facebook Facebook Messenger Google data sources[3] Instagram LinkedIn OkCupid Twitter Telegram VK
Windows 10	Chrome Firefox		
MacOS Sierra 10.13	Safari Chrome Firefox		

[1]For Windows 10, OneDrive file system integration in Windows OS is supported, but Microsoft Store OneDrive application is not supported.

[2]Skype for Business is currently not supported.

[3]The following Google data sources are currently not supported: Chrome, Hangouts, Passwords and Takeout

8.3.3. Content categories

- **Messages:** Communication generated by a user. A message may include text, image, video, files, location information, and tagging data.
- **Images:** Images uploaded by the user that are not attached to message. An image may contain additional properties such as "created at location".
- **Videos:** Videos uploaded by the user that are not attached to message. A video may contain additional properties such as "created at location".
- **Files:** Image or video files uploaded by the user that are not attached to a message.
- **Contacts:** Other people that the subject is in contact with.
- **Calls:** Phone call logs between parties.
- **Location:** Standalone location information not attached to a message, image or video.
- **User profile:** Information about the user such as frequently used devices, bio and home town.
- **User activity:** Activities performed by the user. The type of activity will depend on the application, and may include web searches, web pages navigation, voice commands, calendars, reminders, notes, travel information and history of online purchases.
- **Backups:** Content or device backups stored in the cloud.

UFED Cloud also extracts embedded data artifacts. Examples include email message attachments and the location at the time a Facebook post was made.
Location information is often secondary to the main content category. For example, a journey of a drone on DJI 4 Go or of an Uber passenger will be found under user activity, rather than location.

8.4. Troubleshooting

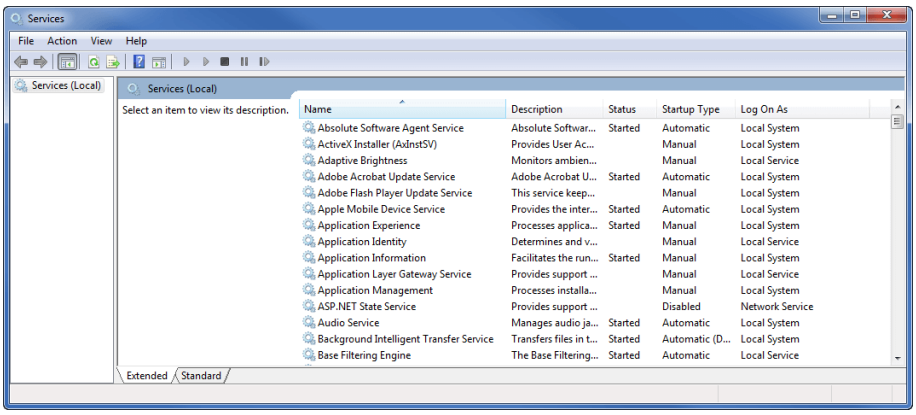
8.4.1. Restarting the UFED Cloud Communication Manager Service

The UFED Cloud Communication Manager service is a computer process that runs in the background and provides communication support to the UFED Cloud application. If a service is not available, a message is displayed while using UFED Cloud. You will need to exit the application, restart the service manually and then start the application again.

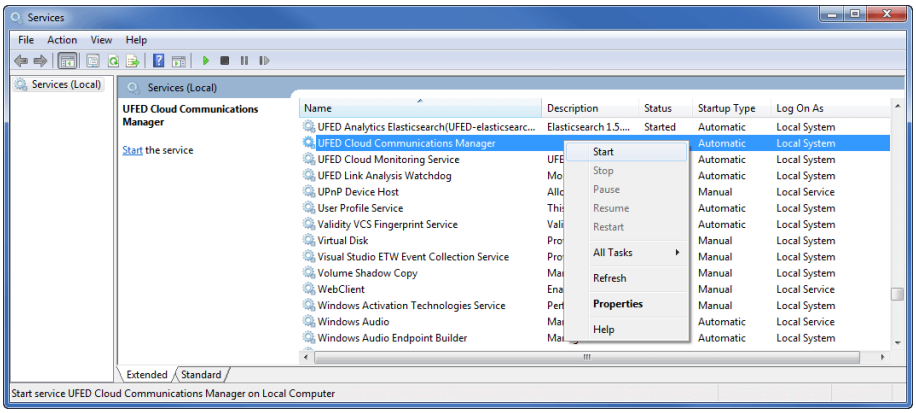
> You must be logged in as an administrator to start or disable services.

Procedure

1. Open the Start Menu, type `services` in the search box, and then click **Services** (or **View local services** for Windows 10). The following window is displayed.



2. Select the UFED Cloud Communication Manager service.
3. Right-click the service and click **Start**.



4. Restart UFED Cloud.

8.0.1. Known issues and limitations

Area	Description	Detected in version
General	The timestamps for Event Logs are only correct according to the date (day) the event occurred. The time displayed is not relevant.	
General	In some instances, the data source do not present the same number of items due to an external issue with the data source itself.	
General	Cloud data extractions are limited to a maximum number of artifacts per type. (If required, the maximums can be changed - contact Cellebrite Support).	
General	Repeating a cloud data extraction that was limited to less than the total existing artifacts may extract different artifacts the next time.	
Snapchat	1. Only "missed calls" are extracted. 2. Only current stories can be extracted. Every story is available for only 24 hours. After that, stories expire and they cannot be viewed and cannot be extracted. Third-party limitation. 3. Messages disappear after they are viewed.	7.9
Instagram	1. Stories are only supported if they have been shared with the extracted account and have not disappeared from the app. 2. Disappearing photos and videos (those marked by a bomb icon) can be extracted as long as they appear in the app. Once they have disappeared from the app, they are no longer available for extraction - only their meta-data is extracted, for example, that user/participant sent a video/image and the timestamp.	7.9
Facebook	Account activity in Facebook is returned from the service with only a date but without a time stamp. UFED Cloud substitutes the missing time stamp with a general filler "00:00" to indicate that the time is unknown. If the user changes the time zone, the time zone change will also take effect on the general filler "00:00" and can change the date accordingly. (For example, the activity listed as 10/06/19 00:00 in a +3 time zone will appear as: 09/06/19 23:00 in a +2 time zone).	7.8

Area	Description	Detected in version
iCloud Web, iCloud WhatsApp - Incorrect credentials	If the wrong 2FA code is attempted multiple times in a short time span, iCloud will stop sending the verification SMS. After 4-5 failed attempts, wait 10-15 minutes before making another attempt.	7.8
Samsung Backup	1. Only the last 1000 calls/SMS are extracted. Third-party limitation. 2. Highly variable data is extracted. Differs greatly by Samsung model and OS version. For example: a. Samsung s7 edge Backup includes calendar and contacts but Samsung A7 does not. 3. In some models, contacts are extracted only if they were saved to the SIM card. 4. In some models, UFDR report does not contain Profile details that contain user profile and WIFI passwords.	7.8
Google Home	Audio files are not returned. Third-party limitation.	7.7
Google Keep	Attached locations are not returned from the server. Third-party limitation.	7.7
Lyft	The map view does not show the ride. This is caused by a third-party limitation as the server does not return coordinates for the pickup and drop-off points. Workaround - addresses are shown.	7.7
Lyft	Canceled rides are automatically deleted after some unspecified time period. Third-party limitation.	7.7
PC login collector	Google Hangouts is not supported.	7.3
Data source: Skype	Records of video calls are not extracted.	7.3
PC login collector	MAC Twitter tokens are not supported.	7.1
Extractions	Extractions using cookies extract less data than mobile device tokens.	7.0
PC login collector	Internet Explorer 11 is not supported on Windows 10.	7.0
Data Source: VK	When an image has been modified, the date and time of modification is not available.	6.3

Area	Description	Detected in version
Data Source: LinkedIn	UFED Cloud calculates the image hash values from LinkedIn's server. Users see an optimized version of the image which may have a different hash value.	6.2
Data Source: Google Takeout	When the Google account's primary language is not English, the Takeout extraction may appear incomplete.	6.2
Data Source: Google Keep (via Google Takeout)	Drawings contained in Notes are displayed under Images, are not linked to the original note.	6.2
Data Source: Box	Tiff files extracted from Box may appear corrupted when opened in Windows viewer.	6.2
Proxy	UFED Cloud extraction methods may be blocked via proxy. Cellebrite recommends working without a proxy.	6.2
PC Token Extractor	Limited to tokens from Google Chrome browser.	6.1
Data Source: WhatsApp (Google Drive)	xxx.mov video file extention is displayed as xxx.mp4.	6.1
Data Source: WhatsApp (Google Drive)	Restored data contact info is displayed as attached files.	6.1
Data Source: WhatsApp backup (iCloud)	User account packages are not supported. Recovery is limited to media files & attachments; chats are not extracted.	6.1
Data Source: Google 2-factor authentication	iOS account packages including Google 2-factor authentication are not supported.	6.1
Data Source: Telegram	Account packages are not extracted from iPhone.	6.0
Data Source: Facebook	When selecting to exclude attachments not all chat messages are extracted.	6.0

Area	Description	Detected in version
Data Source: Cloud Login Collector	When using the Cloud Login Collector to collect tokens from iOS 8x and below, the token may expire after a short time.	6.0
Data Source: Google Chrome Sync	Google passwords are not extracted when a Chrome passphrase is defined (will be available via Google Chrome).	6.0
Data Source: Google Drive	The following file types are not extracted: map, presentation, drawing, spreadsheet, document, form and crypt8.	5.2
Data Source: VK	Posted videos with privacy not set to "All Users" are not extracted.	5.2
Data Source: Twitter	Cannot import pending follower users that were suspended by Twitter.	5.2
Data Source: WhatsApp Backup	The duration of the selected video is not displayed.	5.2
Data Source: WhatsApp Backup	For group discussions, some system messages such as group name change, group icon change, new party joined may not be displayed.	5.2
Data Source: iCloud Drive	Incorrect file path with right-to-left languages.	5.1
Data Source: One Drive	The modified time displayed may not be correct. It displays the time modified on the server, while the OneDrive UI displays the time modified on the client.	5.1
Data Source: iCloud	Occasionally an extraction is completed with errors, because it could not download devices and locations. To resolve this issue try performing the extraction again.	5.1
Data Source: iCloud	Extraction from iCloud email via IMAP is case sensitive. The user name must be entered correctly.	5.1
Data Source: Google Search History	The user profile information is not extracted via credentials or account package.	5.1
Data Source: Google Search History	Voice searches appear as visited pages instead of search requests.	5.0
Data Source: VK	Audio files that were uploaded or attached from the user's PC cannot be extracted.	

Area	Description	Detected in version
Data Source: VK	VK does not generate a unique ID for the post and comments, and therefore it is not displayed.	
Data Source: VK	Comments on images and videos uploaded by the subject on their wall, appear twice.	
Data Source: Google Contacts	Contacts with only a name, without additional data such as phone number, address or email are not extracted.	
Data Source: Facebook	The number of extracted participants for a Facebook event is limited to 6,000.	
Data Source: Facebook	The "Likes" for some user post images uploaded to an album are not displayed.	
Data Source: Facebook	Posts that were merged by the Facebook server are not extracted.	
Data Source: Facebook	People that liked edited comments are not displayed on the right pane.	
Data Source: Facebook	People that liked friend's comments on a user's post are not displayed on the right pane.	
Data Source: Facebook	A post may contain duplicate posts. This is due to an issue in Facebook that miscorrelates comments of one post with another post.	
Data Source: Facebook	Facebook comments on posts of a new image uploaded to an album with "friends only" permission are not extracted.	
Data Source: Facebook	Details of a Facebook event in which the subject is participating, will only be extracted if content (e.g., posts, images, videos) was generated during the selected time frame of the extraction.	
Data Source: Facebook	Facebook posts in which the subject is tagged (or tagged in and shared with friends only) are not extracted.	
Data Source: Facebook	Facebook posts that contain location and attachments (photos, videos, etc.) are displayed in the Timeline View without the attachments. The attachments are displayed as uploaded content in the Files view without the ability to correlate them with the post.	
Data Source: Facebook	Attachments to Facebook comments are not extracted.	
Data Source: Facebook	Deactivated Facebook accounts are not extracted as contacts, although they may appear in the subject's contacts list in Facebook.	
Data Source: Facebook	"Feeling/Activity" information attached to a Facebook post is not extracted.	

Area	Description	Detected in version
Data Source: Facebook	Photos added to the subject's Facebook album by external parties are not extracted.	
Data Source: Facebook	The Facebook video duration property is not extracted.	
Data Source: Facebook	Emotion icons in Facebook chat messages are not displayed.	
Data Source: Facebook	Facebook posts that the subject hides from his/her timeline are not extracted.	
Data Source: Facebook	Facebook locations added by the suspect may not be extracted if the specified location is not known by Facebook.	
Data Source: Facebook	Facebook photos attached to posts are displayed without width and height properties.	
Data Source: Facebook	Facebook chat message categories such as Other, which are filtered from the Inbox, are not extracted.	
Data Sources: Facebook	Facebook "Say Thanks" videos are not extracted.	
Data Source: Facebook	While extracting data from Facebook, the following error messages may be displayed: "The remote server returned an error: (404) Not Found." "The remote server returned an error: (500) Internal Server Error." "The remote server returned an error: (400) Bad Request." "A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond." This may cause some of the information not to be extracted. To resolve these errors run the extraction again.	
Data Source: Facebook	Only a partial list of the posts may be extracted due to a known issue in the Facebook interface: https://developers.facebook.com/bugs/590765867735109/	
Data Source: Facebook	Event log does not show all text (log title).	
Data Source: Gmail	Extraction of locations from attached images in Gmail is not supported.	
Data Source: Gmail	Replied or forwarded email messages that are extracted using an account package from an Android device do not have reference to the original email messages.	

Area	Description	Detected in version
Data Source: Gmail	When using login information from an Android device the CC and BCC recipients are not extracted.	
Data Source: Gmail	Text formatting such as bold or underline is not displayed in email correspondence.	
Data Source: Gmail	Attachments from external sources (e.g., links to a file in Google Drive) are not displayed.	
Data Source: Google Drive	Google Docs files created in Google Drive are extracted with a size of zero, even though the file contains data. Data can still be displayed.	
Data Source: Google Drive	Google map files stored on Google Drive are not downloaded. There is an indication that the map exists.	
Data source: Google Location History	Google Location History is not supported for iPhone 4 regardless of the device extraction method.	
Data source: Google Location History	During the first few days that data is collected, the number of locations presented may change.	
Data Source: Twitter	While extracting data from Twitter, the following error may be displayed: "The remote server returned an error: (404) Not Found." This may cause some of the information not to be extracted. To resolve this error run the extraction again.	
Data Source: Twitter	Twitter extractions are limited to 800 tweets from the home timeline (which contains the user's tweets and the users he/she follows) and 3,200 tweets from the user's timeline (which contains tweets of the user).	
Data Source: Dropbox	Videos uploaded to Dropbox via iPhone are displayed with a duration property of zero.	
Data Source: Dropbox	For right-to-left languages, the file name and directory displayed in the right pane are reversed.	
Discord	There is no accurate indication of how many Participants there are in a channel chat. It will always display '2', the extracted account, and the channel name.	
Discord	No error when using wrong credentials the first time they are entered. Only when entereing credentials on the next screen there will be an indication of incorrect credentials.	
Android backup	Extractions finish with trace error: "No device found for merged project.".	

Area	Description	Detected in version
Android backup	Extraction finishes with the following errors when backup is not accessible: 'Failed to execute: AndroidBackupCloudExtractor' Failed to restore backup'' This will also occur when there were more than one backup, and the other downloaded successfully.	
Android backup	When selecting a data source that contains backup and extracting it with more data, the following error will be displayed: "No device found for merged project."	
Android backup	Can access external apps only on Android 7 and below.	
Data source: Skype	Audio messages on skype are stored on the servers for 30-60 days after they are played.	
Extraction	Deleting the data for an extraction that was stopped by the user, causes some files related to the extraction to remain on the hard drive of the computer. These files are not accessible by the user.	
Extraction	Extraction data may not be recovered if an unexpected error occurred during the extraction. In this case, the best practice is to redo the extraction.	
View	Emails in HTML view in the content pane (right pane) are limited to 1,000 characters. Use the regular view to review large emails.	
Report	Reports cannot be generated when an extraction is taking place. You should either wait for the extraction to complete, or stop the extraction using the Extraction manager prior to generating a report.	

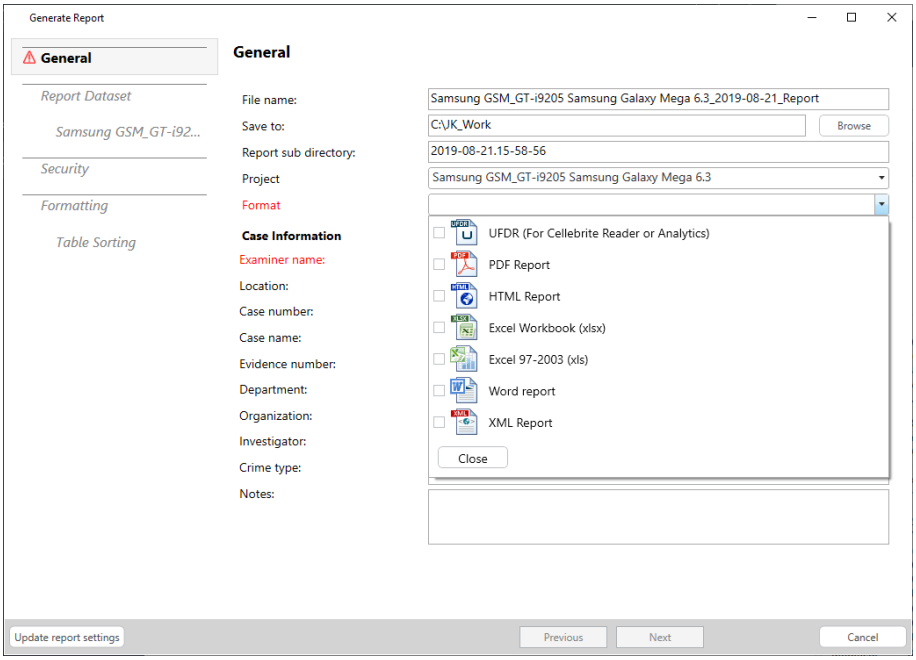
9. Generating a report

You can generate a report of the information in the project. Physical Analyzer provides a report wizard to help you through the steps of creating a report.

To generate a Preliminary device report, see Generating a Preliminary device report (on page 268).

To generate a report, perform the following steps:

1. Select **Report** > **Generate Report** from the application menu. The Generate Report window appears.



2. Enter the relevant information in the **General** fields.

Field	Description
File name	Enter or edit the name for the new report. The default report name is: `project name_date_Report` e.g., `Drone_DJI- Inspire 2_2017-12-25_Report` When more than one project is selected, the default name is: `[Project_name]_date_Report` e.g., `[Project_name]_2017-12-25_Report`
Save to	Enter a location where the new report folder will be created.
Report sub directory	Enter a name for the new sub-folder containing the report(s). The default sub directory name is the current date and time.

Field	Description
Project	Choose the project(s) to include in this report. Only projects that are already opened in Physical Analyzer are available for reporting.
Format	Choose report format(s). If multiple formats are chosen, a report will be generated for each format. Microsoft Excel 2003 reports that contain more than 65,536 rows cannot be opened in their entirety.

Fields in red are mandatory.

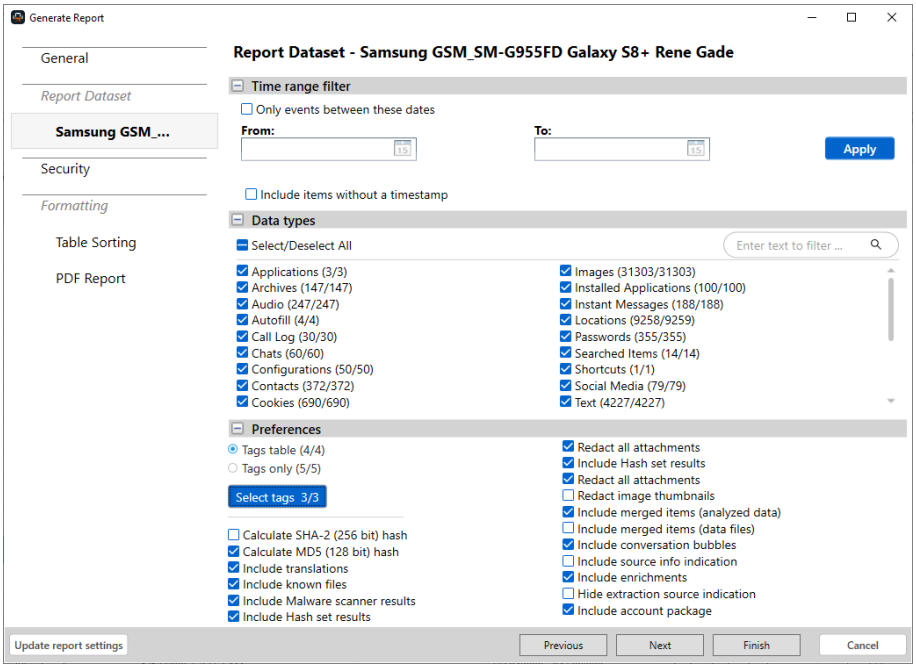
3. Enter the relevant information in the **Case information** fields.

Listed are the default settings for these fields. See Setting the case information (on page 447). See Additional report fields (on page 436) and Report defaults (on page 438) for other defaults. Additionally, the last 10 values entered in these fields are also available in the drop down.

4. Click **Next**. The Report dataset window appears.

9.1. Report dataset settings

The dataset settings enable you to choose events between specific dates and what data to include in the report.



To complete the Report dataset settings, perform the following steps:

1. To use the optional time range filter, in the Report range filter area select the **Include only events between these dates** check box, enter the date range and click **Apply** to update the data in the Extraction area.

> Select the **include items without a timestamp** check box to include events that do not have a timestamp.

2. Under the **Data types** heading, select the analyzed data and the data files to be included in the report.

> The data types listed will vary based on the data available in the selected projects, and include all the data sets listed under Analyzed data and Data types in the project tree.

Next to each data type, the number of items to be included in the report is displayed, alongside the total number of items of this type. The number of items included in the report may change based on your choices in the following sections.

3. Under the **Preferences** heading, select the data to be included in the report.

	Description
Tags table	Select to include tag table in the generated report. To specify which tag labels to include/exclude, click **Select tags**.
Tags only	Select to include tags only (disables all Data types except for Device info) in the generated report. To specify which tag labels to include/exclude, click **Select tags**.
Select tags 3/3	Click to select which specific tag labels you want to include/exclude in your report. This is useful in cases where not all examiners should be exposed to all the tagged items in an extraction.
Calculate SHA-2 (256 bit) hash	Select which calculated MD5 and SHA256 hash keys to add to each Data Files item in the generated report. This selection is for the whole report and applies to all projects within the report. To shorten the report generation process of large projects, do not select the Hash options.
Calculate MD5 (128 bit) hash	
Include translations	Select to include translated text.
Include known files	This option enables you to include system images or files in your report. Clear this option to automatically filter out common/known/system images and save critical investigation time that would otherwise be spent reviewing media images such as device icons, or images that are included by default when installing apps.
Include Malware scanner results	Include results from Malware scanner.
Include Hash set results	Include results from hash databases run on the extraction.
Redact image thumbnails	Select to redact image thumbnails from PDF, Word and HTML reports.
Include merged items - analyzed data and data files	Select to include merged data from the Analyzed data section and/or the Data files section of the project tree. The **Include merged items** options are unselected by default. When these settings are selected, your report will include all items including duplicate items. The total numbers of items selected for the report may change based on these settings.
Include Reader	Select to share UFDR reports with authorized persons using the Reader. The Reader executable will then be included within the report output folder. This option is for the UFDR format only.
Include conversation bubbles	Select to include the chat bubbles of the conversation in the report. To include the metadata of the chat bubbles make sure that the **Include metadata in chat bubbles** check box under **Settings** > **Report Defaults** is selected.

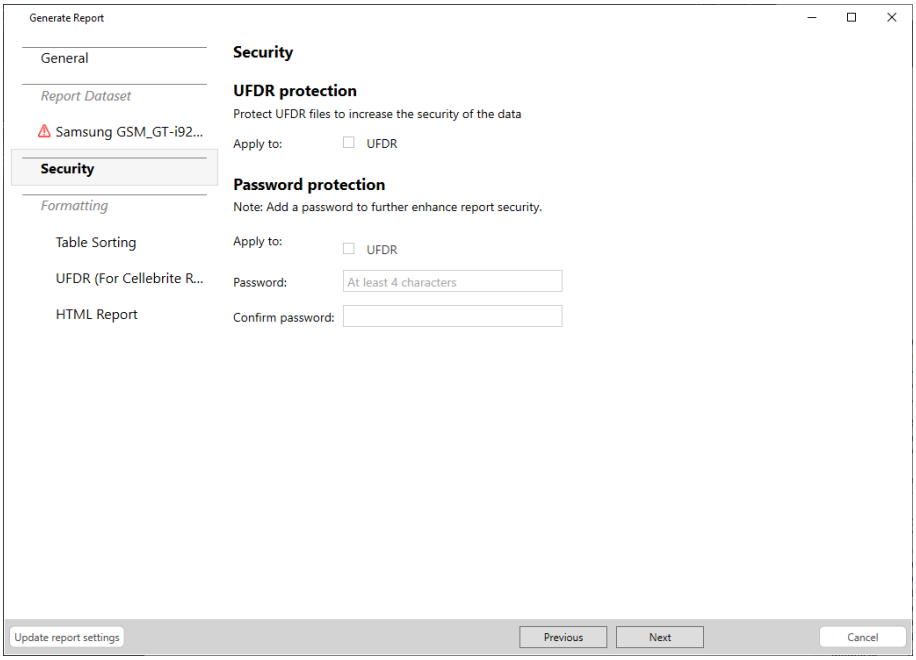
	Description
Include source info indication	Select to include the source file information (as displayed in the Source file information column).
Include enrichments/Review	Select to include BSSID enrichments and Image classification.
Hide extraction source indication	Select to hide extraction source types. If the check box is cleared, the report will indicate the type of extraction from which the field was obtained e.g., physical, logical, file system. If the check box is selected, the type of extraction will not be displayed. The check box is only relevant with the Multiple extraction feature. For single extractions, the extraction source type will not be displayed.
Include account package	Select to include an account package, which is an export file that contains user credentials.
Include Activity sensor data samples	Select to include the sample data of all detailed measurements of the activity data.

4. Click **Next**. The **security** screen appears.

9.2. Report security settings

The report security settings includes two levels of protection:

- **UFDR protection:** UFDR files hold sensitive, confidential and personal data. Adding this optional security layer enables you to better protect data contained in UFDR files. The Reader and Cellebrite Pathfinder solutions can automatically read UFDR files, even if the security layer is selected. If you are importing UFDR files into third-party tools, you should not select this option.
- **Password protection:** Apply password protection to Excel, PDF, UFDR, and Word reports.

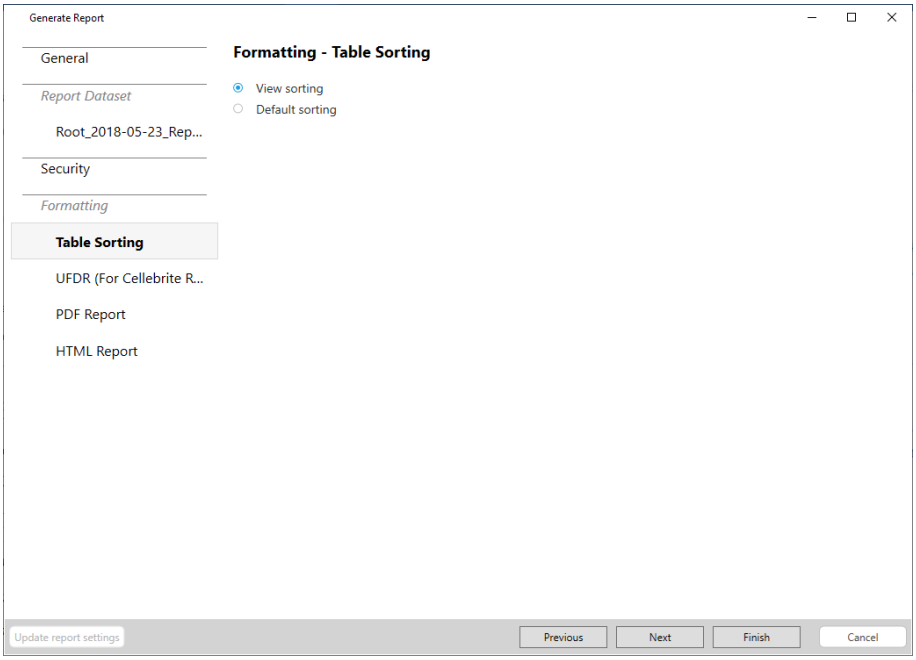


To complete the security settings, perform the following steps:

1. Select the **UFDR** check box if you would like to protect the UFDR file.
2. Choose the report formats to protect with a password (optional).
3. Enter and confirm the password.
4. Click **Next**. The **Layout** screen appears.

9.3. Report layout settings

You can set the report layout to meet your agency's requirements.



To complete the layout settings, perform the following steps:

1. Select **Default sorting** to sort the items included in the generated report according to the default sorting set by Cellebrite for each of the Analyzed and Data file types, or clear **Default sorting** to sort the items according to the selected sorting field and the sorting order (ascending or descending) that was set by the user in each of the data display tables.
2. For each format chosen for this report, you can specify report parameters as follows:

Parameters	Description
Disable models categorization	Select to disable the separation and generate a report in which every data item is generated as a single section without subcategories separation. By default, a categorized report in which each category in the data items group is generated as a separate section in the report is generated. For example, when generating a report with Call logs, select the check box to generate the Call logs as a single list, or clear the check box to break it to a separate list for each category of Call logs.
Logo Header	Text area where you can enter and format custom text to appear in the report header before the logo image.
Logo	Click **Select Image File** to add the logo image to appear in the report header. Supported file formats are: BMP, JPG, GIF, and PNG.

Parameters	Description
Logo Footer	Enter and format custom text to appear in the report footer after the logo image.
Show totals for items not in the report	Add a Total column to the report that displays the total number of items that were excluded from the report.
Show extended deleted state	Include the state (Intact, Deleted, or Unknown) of deleted items in the generated report. When not selected, logs only the state of deleted items as Yes, and is left empty for other states.
Number of lines for email preview	Set the maximum number of lines from each email message to appear in the report.
Display full email body	Display the entire message body.
Number of messages per chat	Set the maximum number of messages per chat message to appear in the report.
Display all chat messages	Display all chat messages in the report.
Font Family	For PDF reports only.
Split HTML report	Ensure that each section of the report starts on a new page. For HTML reports only.
Unprintable characters placeholder	Set the placeholder character to replace the unprintable characters. For Excel and ODS reports only.
The Excel report is compatible with OpenOffice	Select to ensure the Excel report can be opened in OpenOffice. For Excel and ODS reports only.
Generate Contact Identification Data	Select to add a sheet to the Excel report that provides a list of unique contacts based on type. For Excel and ODS reports only.

The parameters displayed will vary based on the report types you have chosen.

3. Click **Finish**.

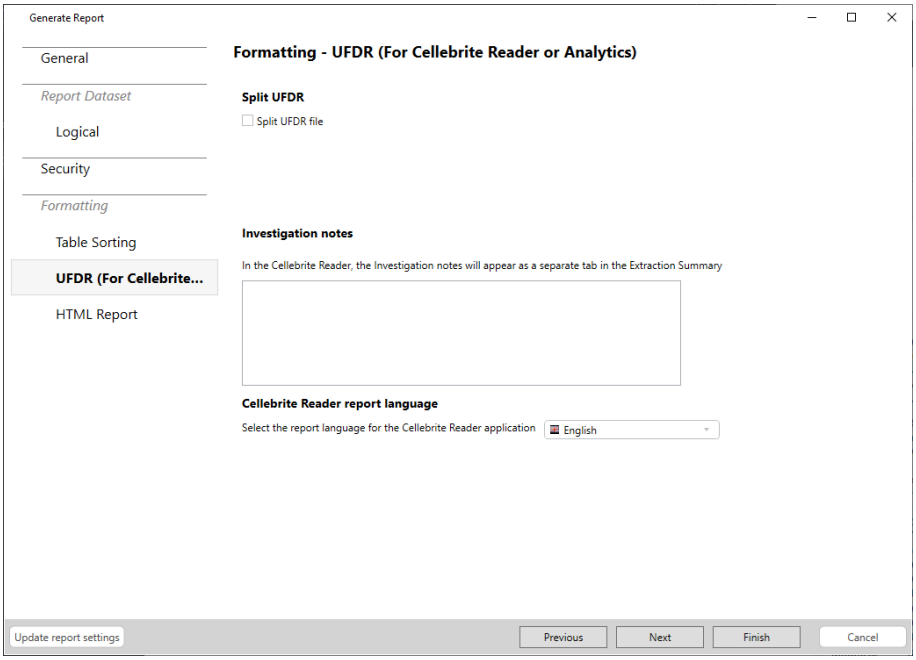
Finish is unavailable until all the required fields are filled. A yellow warning icon is displayed next to all required fields that are not yet complete.

4. When the report is successfully generated, you are prompted to open the generated report file. The file opens using the associated application to the file format installed in the workstation.

> Once a report has been generated for the project, it can be accessed from the Reports section in the project tree. Double click on any of the generated reports to open it in the associated application installed in the workstation. Right click any of the generated reports to open the report file, or select **Open containing folder** to browse the files and folders of the report.

9.3.1. Formatting the UFDR file

This window enables you to split the UFDR file and add investigation notes.



9.3.1.1. Splitting the UFDR file

Splitting a UFDR file enables you to divide a file (too large to fit onto storage media) into multiple smaller files, for easy transfer. Select 700 MB for CDs, 4.7 GB for DVD, or a custom file size between 100 MB to 10 GB. When you open the UFDR that has been split into separate files, Physical Analyzer will automatically merge all the files into a single report.

To split the UFDR file:

1. Select the **Split UFDR file** check box.
2. Select the required file size.
3. Click **Next**.

> To open the split UFDR in Physical Analyzer select the main UFDR file (*.ufdr).

9.3.1.2. Adding investigation notes

If required, enter notes in the area provided. These notes will be displayed as a separate tab in the Cellebrite Reader, under the Extraction Summary.

9.3.1.3. Cellebrite Reader report language

In some cases, UFDR reports are shared with colleagues that need to review it in a different language. You can set the default interface language when opening a UFDR report. This allows the Cellebrite Reader to load in the predetermined language without the need to configure this in the Settings screen. The setting is stored for any UFDR that is created. In Cellebrite Reader a message will be displayed if the report language is different from the application.

9.4. Generating a Preliminary device report

Generate an 'at a glance' intelligence report that includes parsed device information and user account information. Such reports can be used as a quick reference for the lab, prosecutors, and investigators.

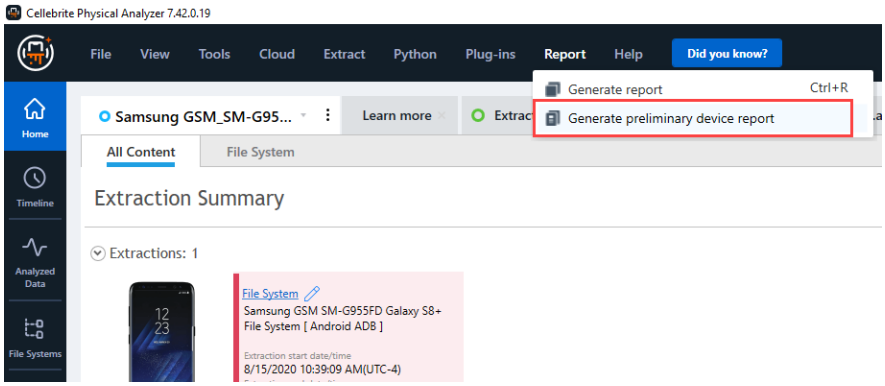
This report includes the device info and a hybrid of the data in the User accounts. This useful 'at a glance' data can inform the investigation units about where other 3rd party evidence may reside and identify if accounts known to the investigation are still on the device.

This PDF report can be emailed to the investigation unit as soon as Physical Analyzer has finished loading the extraction.

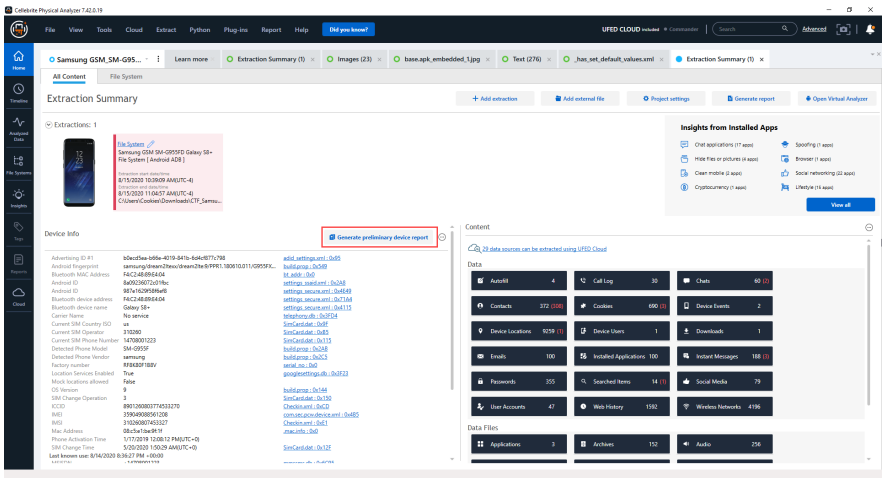
To generate a Preliminary device report:

There are two ways to generate this report:

» From main menu, select **Reports > Generate preliminary device report**.



» In the Extraction summary click **Generate preliminary device report.**



The PDF report will be generated and stored to the default reporting path location.

10. Performing extractions

In Physical Analyzer, perform device extractions in the following ways:

1. For iOS devices, perform physical extraction, file system extraction or Passcode recovery from the device using the iOS device extraction application.
2. For GPS or mass storage, perform an extraction via Physical Analyzer.

10.1. Extraction from iOS devices

Perform a physical extraction from an iPhone, iPod, or iPad device, using the iOS Device Data Extraction wizard.

Prerequisites

To perform an extraction from an iOS device, you will need:

- Physical Analyzer installed on a PC.
- UFED Cable Number 110 or UFED Cable A with Tip T-110 or Apple 30 pin USB cable supplied with the device.
- UFED Cable Number 210 for iOS logical extractions from iPhone 5, iPad Mini and iPad4.

> Extraction from iOS devices is not supported in Virtual Machine environments.

In addition, an Internet connection is required the first time you run iOS device extraction in order to download the necessary support package. Alternatively, the support package can be downloaded using a different computer and copied manually to the computer running iOS device extraction. iOS device extraction automatically notifies you when a software update is available.

> iOS calendar events with a year value of 1604: In general, a calendar entry needs to have a year value, so, when it does not, the timestamp is automatically populated with the default year of 1604. Why 1604? Because it is unlikely that a 21st century user will have any event which happened in 1604 in their calendar, so it is a good indicator of a timestamp without a year. This is a leap year, so if the timestamp falls on 29 February, it will still be supported. 1604 was before the Julian-Gregorian calendar switch.

10.1.1. Physical extraction

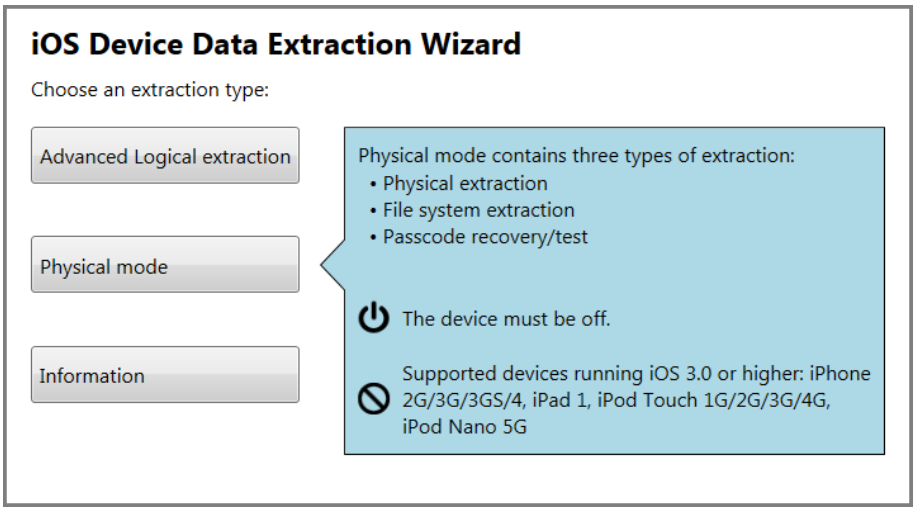
Perform physical and file system extractions for iOS devices.

For a complete list of supported devices, refer to UFED Phone Detective or the UFED Supported Devices document in MyCellebrite.

> This feature is available with Physical Analyzer only.

10.1.1.1. Performing physical extraction from non-encrypted iOS devices

1. Select **Extract > iOS device extraction** or click to start iOS device extraction.



2. Click **Physical mode**.

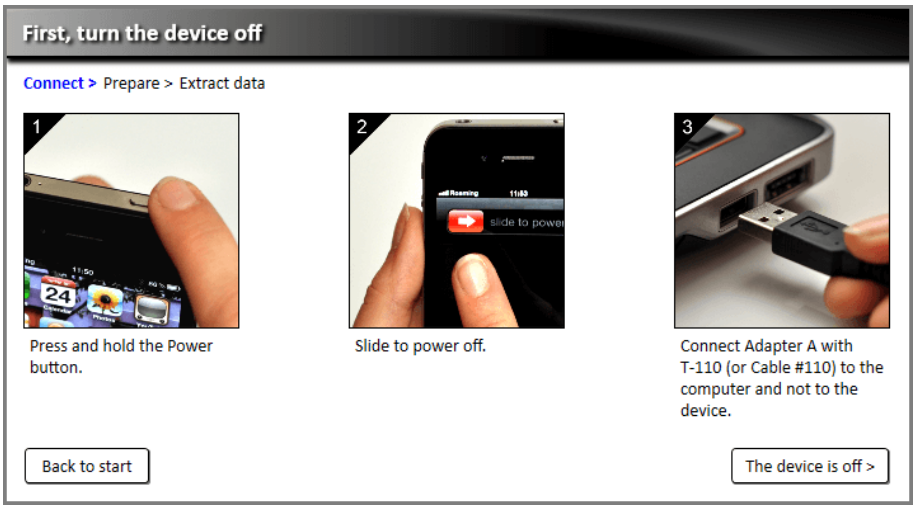
   The first time that you run iOS device extraction, or when a new support package is available, you are prompted to download the iOS Device Support Package. The support package contains the latest utilities that enable iOS device extraction to work with a variety of devices and iOS versions. Depending on your Internet connection, the download may take some time.

   Click **Install** if the computer running Physical Analyzer has an Internet connection.

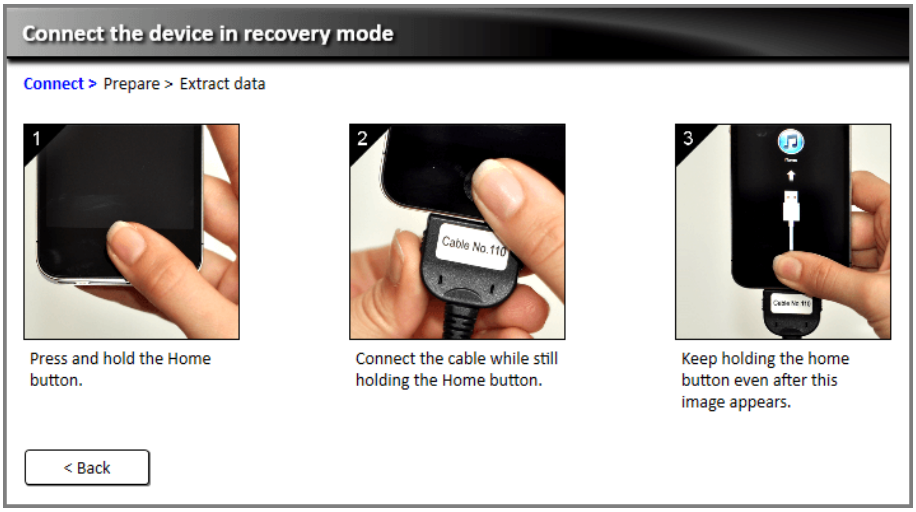
   If your computer is unable to connect to the Internet use a computer with an Internet connection to download the latest support package file as follows:

   a. Go to community.cellebrite.com
   b. Download the support package file called iOS Device Support and save it to the computer running the Physical Analyzer.
   c. When prompted to install the support package, click **Install from file**, then navigate to the location of the support package file, and click **OK**.

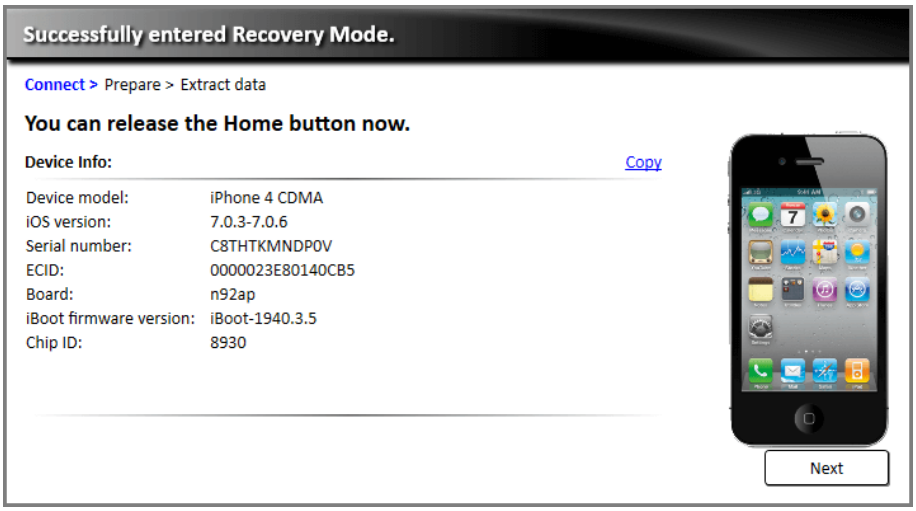
3. Follow the displayed instructions to power off the iOS device and then click **The device is off**.



4. Follow the displayed instructions to activate the iOS device in **Recovery Mode**.



The process automatically continues to the next step.

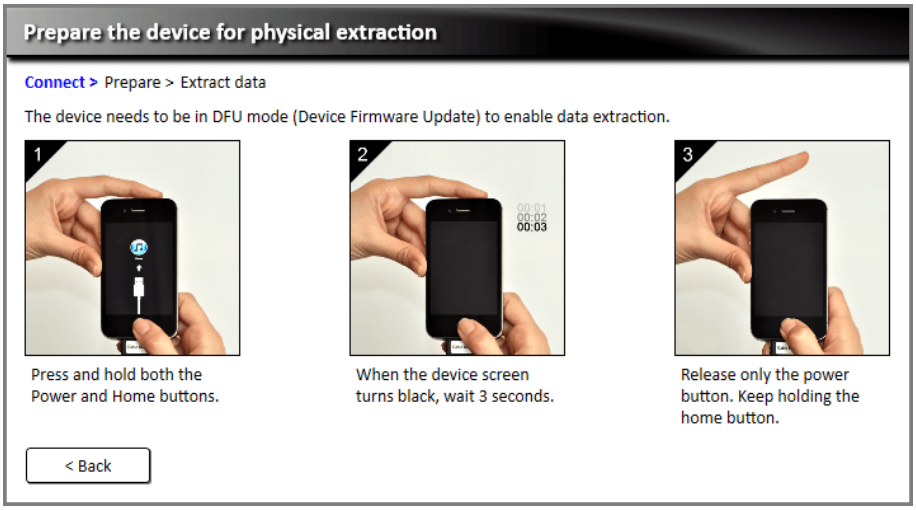


After a device in **Recovery Mode** is detected, iOS device extraction displays some device information, such as serial number, hardware version, iOS version and more.

5. If you need this information, click **Copy** to copy the device information to the clipboard.

> When a range of versions are displayed, the version of the device may be any version within the displayed range. For example, if the version shows **4.0-4.0.2**, the actual version can be 4.0, 4.0.1 or 4.0.2.

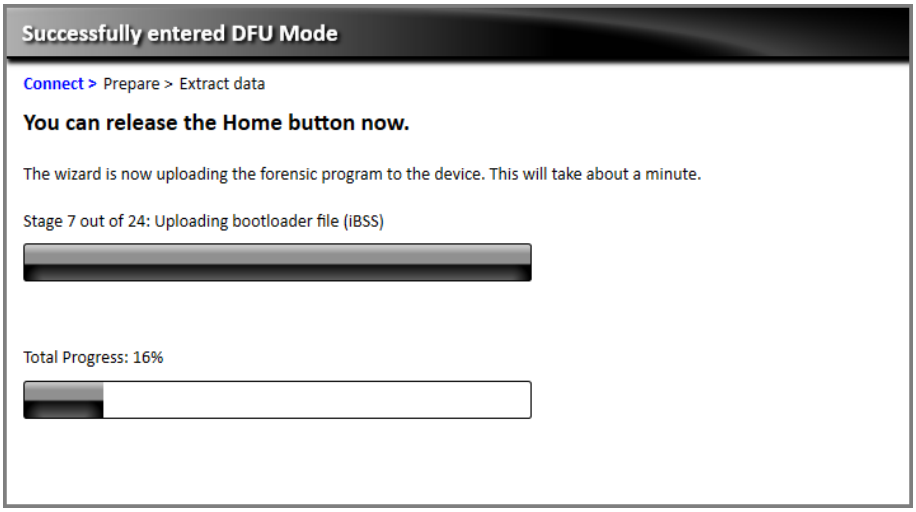
6. Click **Next** to continue.
7. Follow the displayed instructions to set the device to DFU (Device Firmware Upgrade) mode.



iOS device extraction does not affect the device firmware or user data.

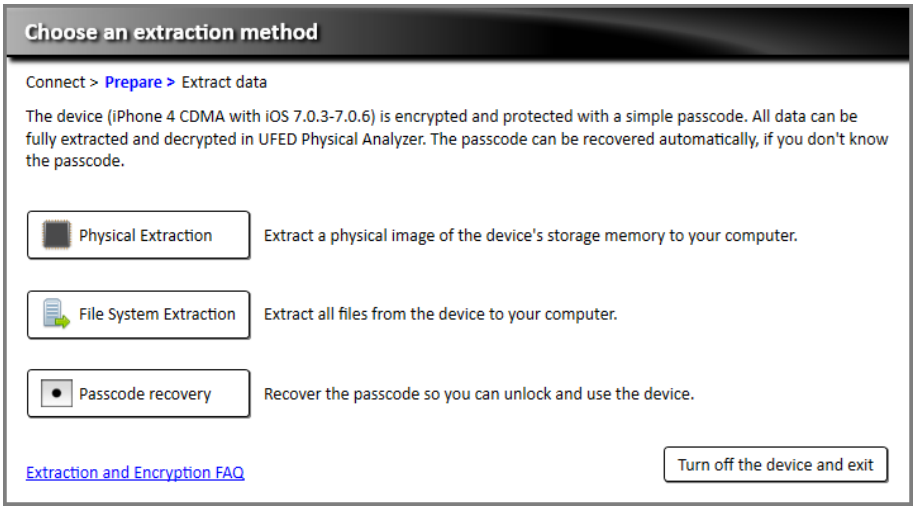
> This step requires precise timing. If the device accidentally turns on, disconnect it from the cable, turn it off, then go back to step 4.

When the device is in DFU mode, a forensics program required for the extraction automatically uploads to the device.

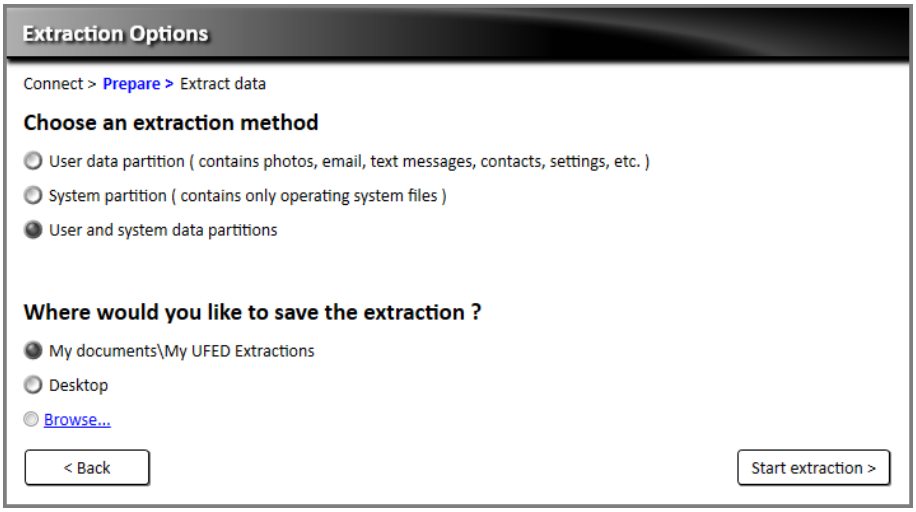


The device is now ready for extraction.

8. Choose the desired extraction type.



9. Choose the desired extraction method:
   - For Physical Extraction: **User data partition**, **System partition**, or **both**.
   - For File System Extraction: **User data partition** or **both**.
10. Choose the **location** to which to save the extracted data. You can save it locally on the computer or to any removable storage device.



11. Click **Start extraction** to continue.

> If the device is locked with a passcode, see Performing physical extraction from encrypted devices (below).

12. Wait for the extraction process to complete.

    The duration varies depending on the extraction method, the device model, the amount of data on the device, the extracting computer, and other parameters.

    The following options are available at the end of the extraction process:

    - **Open in Physical Analyzer** – Loads the extraction file in Physical Analyzer.
    - **Open file location** – Opens the folder that contains the extraction files.
    - **Turn off the device and exit** – Turns off the device and sets it back to normal mode.
    - **Back to extraction options** – Returns to the extraction methods screen (step 8).
13. Turn off the device and set it back to normal mode.

10.1.1.2. Performing physical extraction from encrypted devices

iOS device extraction can extract data from encrypted devices. The amount of data that can be extracted depends on the type of passcode the device is locked with.

There are two kinds of passcodes:

- Simple passcode – 4 digits from 0 to 9 (e.g. 1234, 8787, 2580, etc.)
- Complex passcode – Any combination of numbers, letters and symbols (e.g. 93qP@Mv, iLoVeYoU, etc.)

The decryption process happens in Physical Analyzer and not during the iOS device extraction. Most data, such as contacts, messages, photos, some emails, and more, can be decrypted without knowing the passcode. However, to decrypt some of the saved passwords and emails, you need to know the device passcode.

If the device is locked with a simple passcode, iOS device extraction automatically recovers the passcode for you. If the device is locked with a complex passcode, you can manually try as many passcodes as you like, or continue the extraction without being able to decrypt some of the saved passwords and emails.

If the device isn't locked with a passcode, all data is extractable – even if the device is encrypted.

10.1.1.2.1. Extracting data from a device with a simple password

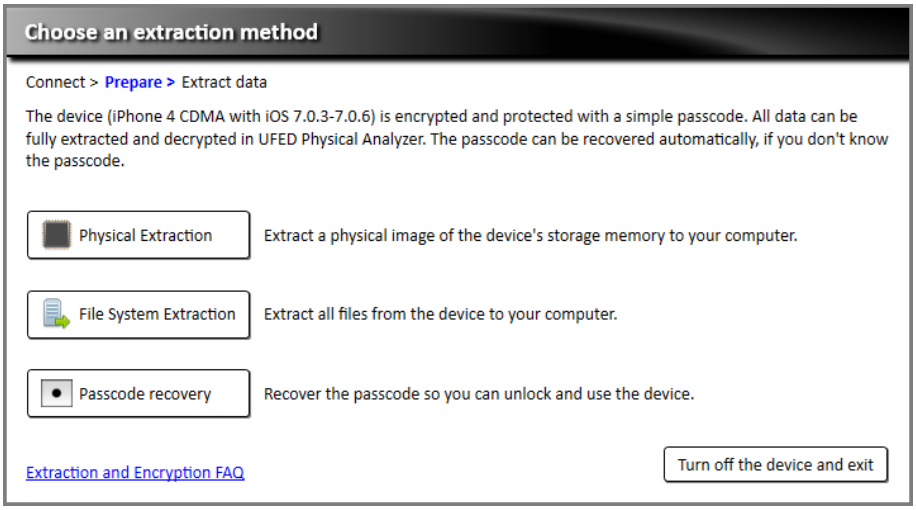
1. Perform steps 1-7 of Performing physical extraction from non-encrypted iOS devices (on page 270).

   When the device is ready for extraction (step 8), an additional **Passcode Recovery** option is added to the two extraction options (**Physical Extraction** and **File System Extraction**).

   The Passcode recovery option provides the device passcode so you can unlock and use the device.

2. To extract and recover the passcode in a single process, choose **Physical Extraction** or **File System Extraction**.

   The following steps demonstrate a physical extraction process (starting at Performing the Data Extraction), but they are the same for a file system extraction.



3. Click **Physical Extraction**.
4. Choose the partition you wish to extract, and the location where you want to save the extraction, then click **Next**.
5. If you don't know the passcode, click **Recover the passcode for me** to recover the passcode prior to the extraction.
6. If you know the passcode, enter it in the text box field below. A check mark verifies if the correct passcode was entered.
7. Click **Continue**.

   The extraction process starts.

10.1.1.2.2. Extracting data from a device with a complex password

1. Perform steps 1-7 of Performing physical extraction from non-encrypted iOS devices (on page 270).

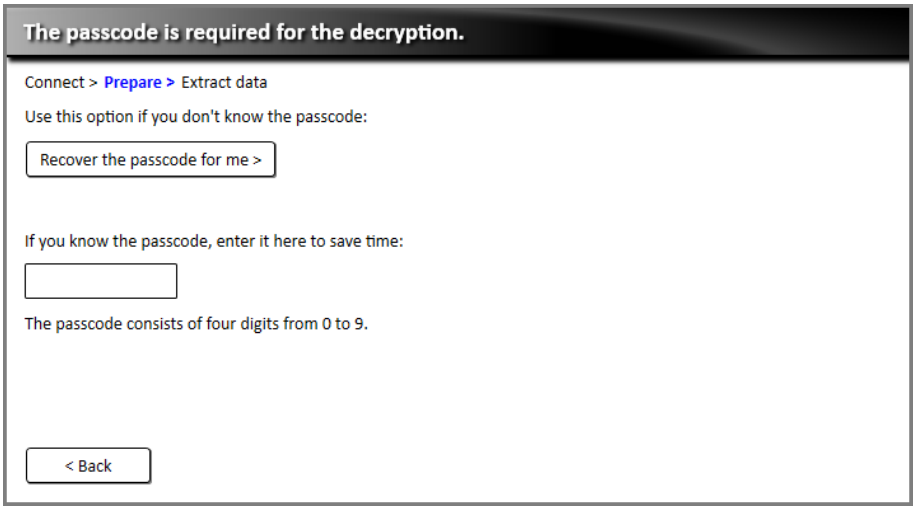
   When the device is ready for extraction, an additional **Passcode Recovery** option is added to the two extraction options (Physical Extraction and File System Extraction).

   Use the **Test Passcodes** option to test and verify as many passcodes as you like in real time. iOS device extraction cannot recover a complex passcode.

   Most data is decrypted in Physical Analyzer, but some of the saved passwords and email files are not decrypted unless the complex passcode is known.

   The following steps demonstrate a physical extraction (starting at Performing the Data Extraction), but they are the same for a file system extraction.

2. Click **Physical Extraction**.
3. Choose the partition you wish to extract and the location to which you want to save the extraction, then click **Next**.



4. Do one of the following:
   - If you know the complex passcode, enter it manually. If you do not know the complex passcode, be aware that some data cannot be decrypted by Physical Analyzer.
   - Use the text field to test as many passcodes as you like without locking the device. A check mark appears when you enter the correct passcode.
5. Do one of the following:
   - To start the extraction with the complex passcode, click **Continue >**.
   - To start the extraction without the complex password, click **Continue without passcode**.

   The extraction process begins.

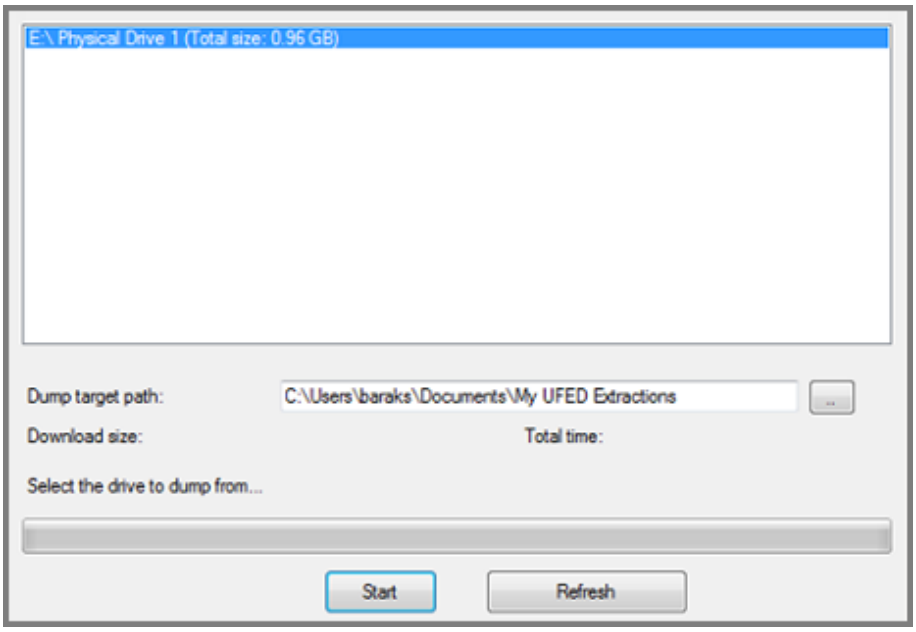
10.2. Extraction from GPS or mass storage devices

Extract and save data from a GPS device (Gamin, Mio, and TomTom) or a mass storage device.

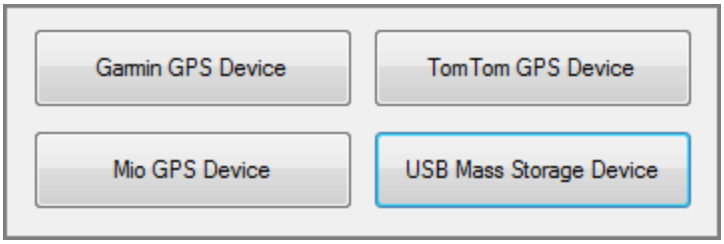
> Only administrator users can read data from GPS devices. If you are not logged in as an administrator, close Physical Analyzer, right-click the Physical Analyzer icon on your desktop, and select **Run as administrator**.

> This feature is available with Physical Analyzer only.

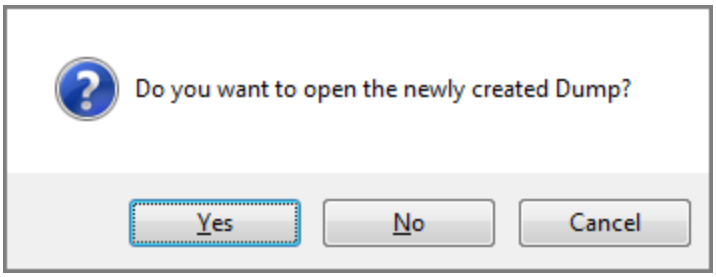
1. Connect the GPS or mass storage device to your PC.
2. Select **Extract** > **Extract GPS/mass storage device**. The following window appears.



3. Select the device.
4. Do one of the following:
   - Enter the path where you want to save the data extracted from the device.
   - Click ..., and browse to and select the desired location.
5. Click **Start**.



6. Select the type. The extraction begins. When finished, the following message appears:



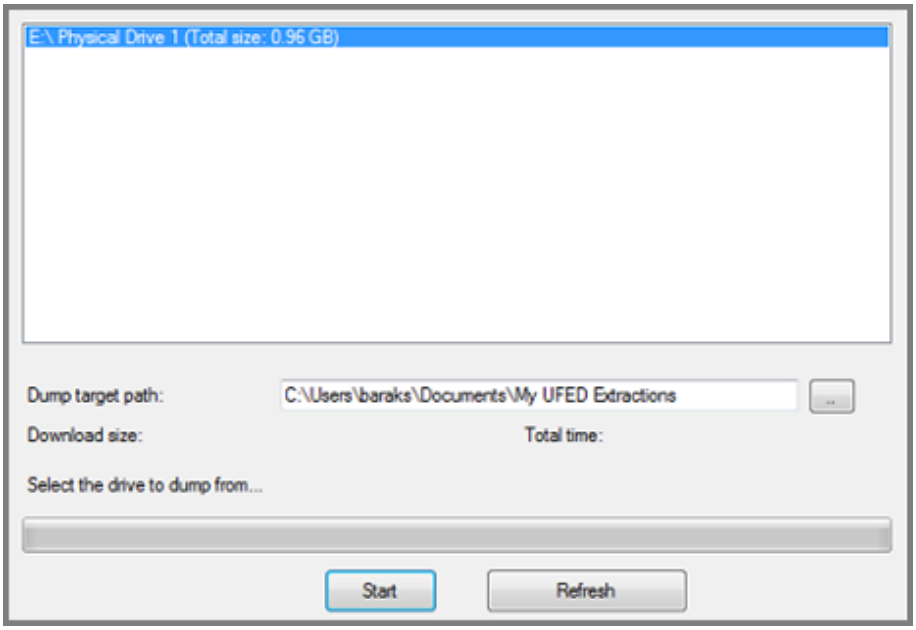
7. Click **Yes** to open the extraction.

10.2.1. Reading data from a GPS or mass storage device

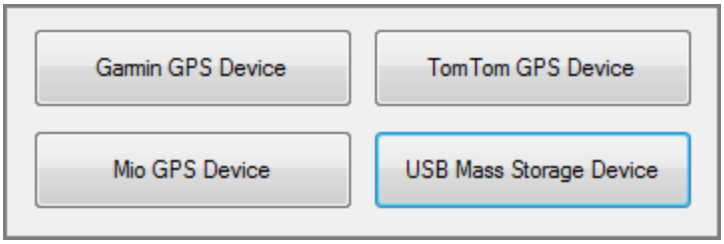
Read and save data from a GPS device (Gamin, Mio, and TomTom) or a mass storage device.

> Only administrator users can read data from GPS devices. If you are not logged in as an administrator, close Physical Analyzer, right-click the Physical Analyzer icon on your desktop, and select **Run as administrator**.

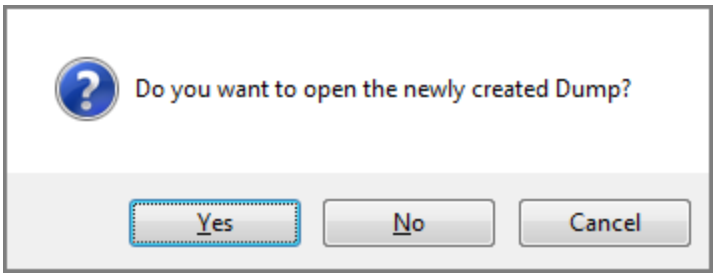
1. Connect the GPS or mass storage device to your PC.
2. Select **Tools** > **Dump GPS/Mass Storage Device**, or click .



3. Select the device.
4. Do one of the following:
   - Enter the path where you want to save the data extracted from the device.
   - Click ..., and browse to and select the desired location.
5. Click **Start**.



6. Select the dump type. The extraction begins. When finished, the following message appears:



7. Click **Yes** to open the extraction.

11. Advanced features

This section describes some advanced features of Physical Analyzer such as:

11.1. App insights 281

11.2. AppGenie 285

11.3. Virtual Analyzer 288

11.4. Accessing public data 300

11.5. SQLite wizard 307

11.6. Fuzzy models 330

11.7. Generating dictionary files 333

11.8. Working with TomTom 334

11.9. Opening an encrypted extraction 336

11.10. Opening an encrypted zip file 338

11.11. Extraction and decryption of BlackBerry backup files 339

11.12. WhatsApp decryption on BlackBerry databases 340

11.13. Exporting an account package from Physical Analyzer 345

11.14. Media classification 346

11.15. Selective apps decoding 353

11.16. Carving images 357

11.17. Carving locations 361

11.18. Generic file carver 363

11.19. Verifying hash values 364

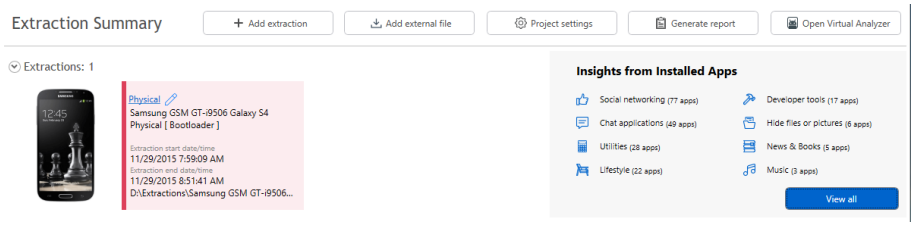
11.20. Accessing WhatsApp Web data 365

11.21. Network dongle – admin procedures 369

11.1. App insights

Browse the apps on the device sorted by category and select the apps for which you require additional data. Each category includes a list of related apps. The categories include store categories from Google Play and Apple App Store, as well as important categories defined by Cellebrite e.g., Hide files or folder (for suspicions apps) and Spoofing. Internal application services are not displayed in this view.

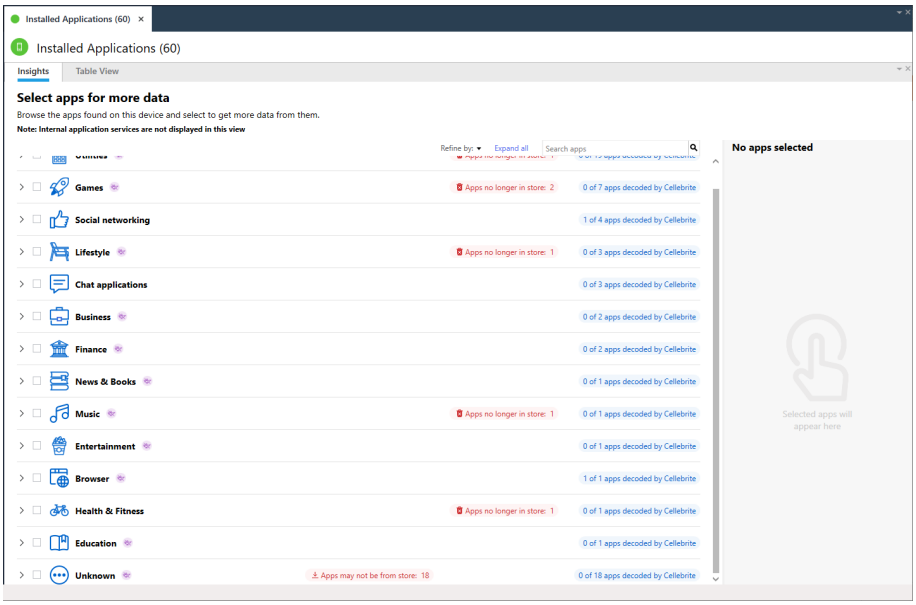
11.1.1. Extraction summary



In the extraction Summary, you can see a snapshot of the app categories and the number of apps in each category. To see all the installed applications, click **View all**.

11.1.2. Installed Applications

From the Insights tab, you can browse the apps on the device sorted by category and select the apps for which you require additional data.



This view shows all the categories found on the device. You can select an entire category with all the apps or browse and select individual apps. It also includes Apps that may not be from the store i.e., could be installed from other sources besides the actual official apps stores (

Apps may not be from store: 18), apps that are no longer available in the app store (Apps no longer in store: 1) as well as how many apps in the category were successfully decoded (6 of 19 apps decoded by Cellebrite).

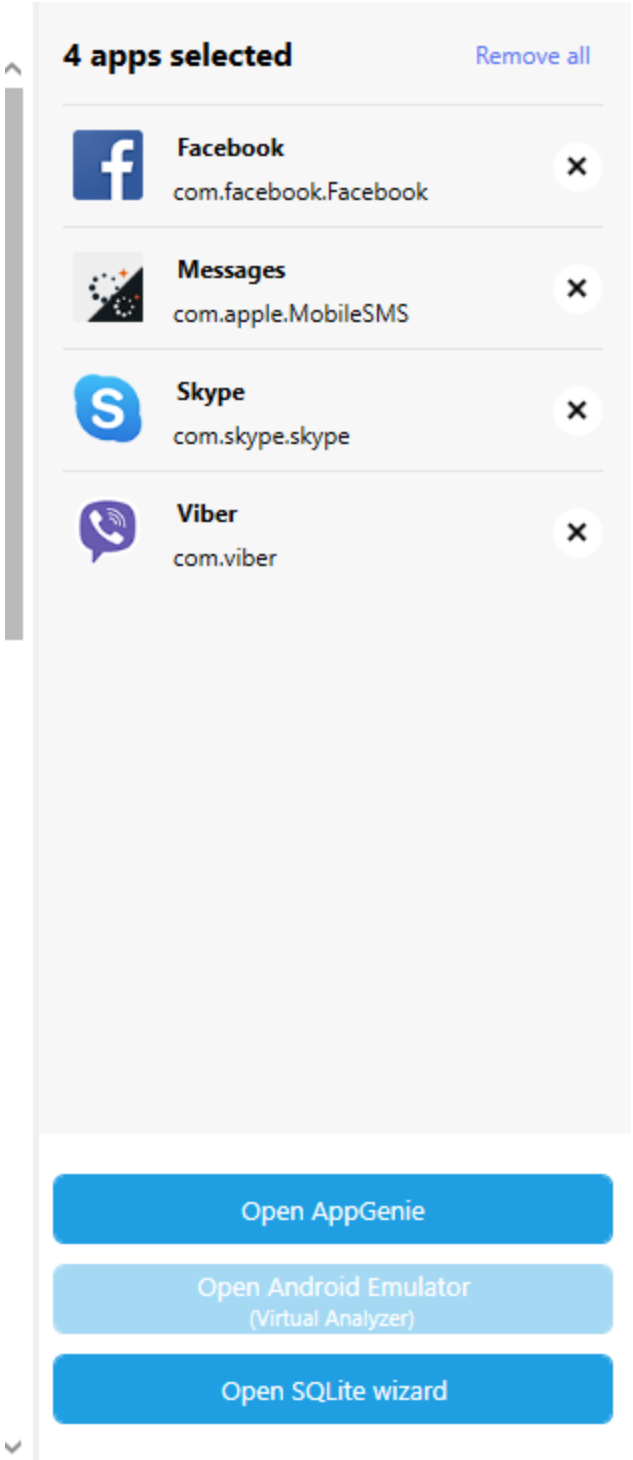
The following table explains the icons and fields displayed in the window.

11.1.2.1. App actions

Icons and fields	Description
	Apps that were decoded by Cellebrite.
	Generic Cellebrite representation of the app. If possible, app icons are displayed from Google Play or the App Store.
	Apps that the user installed and are no longer available in the store.
	Categories where apps are not supported by AppGenie by default. You can change this limitation in the settings window (**General Settings** > **Decoding**).
	Click this image next to each app to view a description of the app as it appears in Google Play or the App Store. The first 500 characters are displayed.
Refine by	You can filter the apps by selecting the following options: » **Emulatable apps:** Only show apps that can be emulated by the Virtual Analyzer. » **Not decoded by Cellebrite:** Only show apps that were not decoded by Physical Analyzer. Click **Clear filters** to rest the filters.
Search apps	Enter text to find the app.
Expand all *Collapse all*	Expand or collapse all the apps in each category.

To get more data from apps:

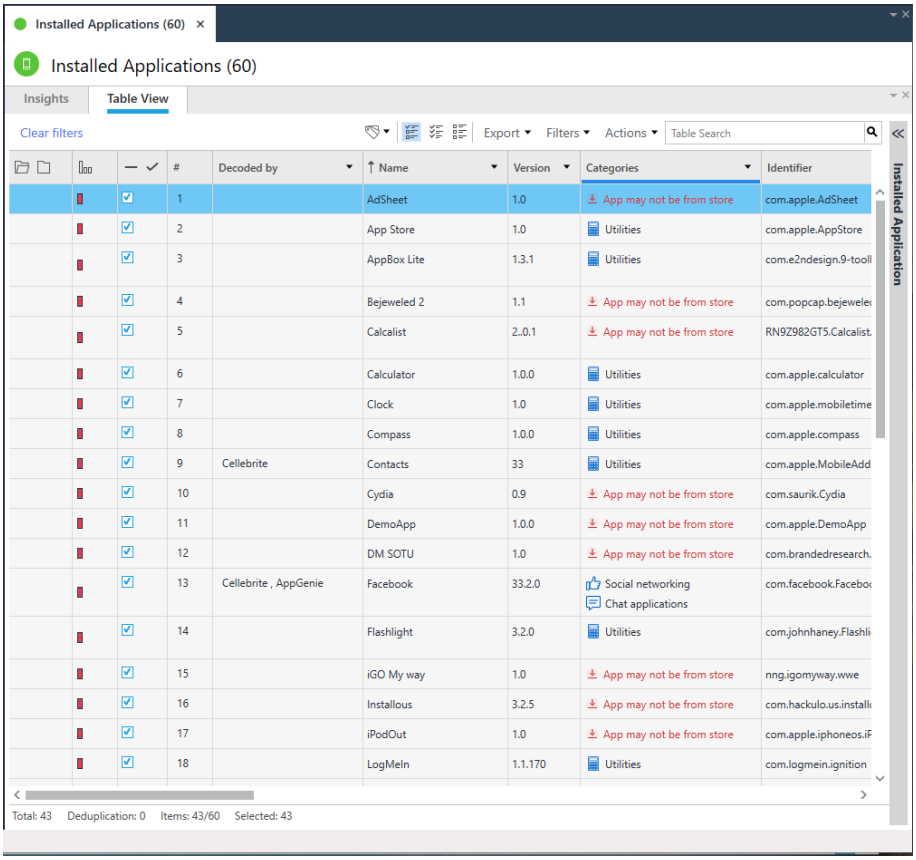
1. Select the required apps. The selected apps appear in the area on the right.



2. To get additional information select the tools you would like to run. Select from the following tools (the tools are not applicable for all apps):

- **AppGenie:** App Genie is a research tool that provides additional app data such as Contacts, User accounts and Chats. The tool's availability depends on the selected app categories. You can change this limitation in the settings window (**General Settings** > **Decoding**). For more information, see AppGenie (on the facing page).
- **Virtual Analyzer:** This tool is only enabled for Android devices. Additionally, a maximum of 5 apps can be selected and these apps must support emulation. For more information, see Virtual Analyzer (on page 288).
- **SQLite wizard:** This tool is only enabled for applications with databases. For more information, see SQLite wizard (on page 307).

11.1.3. Table view



From the Table View tab, you can view the applicable categories for each app or if the app may not be from the sore. You can also filter the table by category. The decoded by column indicates if the app was decoded by Celllebrite and/or a tool such as AppGenie, Virtual Analyzer or the SQLite Wizard.

Switch to the Table view to see a list of installed apps and their categories

11.2. AppGenie

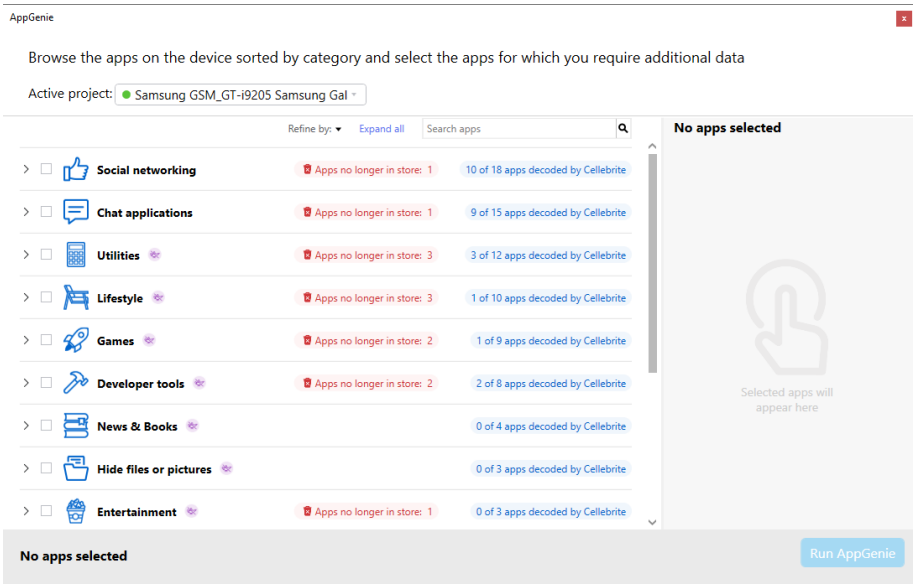
AppGenie is a research tool that tries to automatically identify specific artifact types from device databases. AppGenie analyzes databases based on past decoding support, heuristics and can provide additional app data such as Contacts, User accounts, and Chats.

As a research tool, the suggested results do not replace native Physical Analyzer decoding and should be used as preliminary/triage results for manual review, because it may include false-positives and partial results. It's recommended to review results before including them in your reports.

To run the AppGenie:

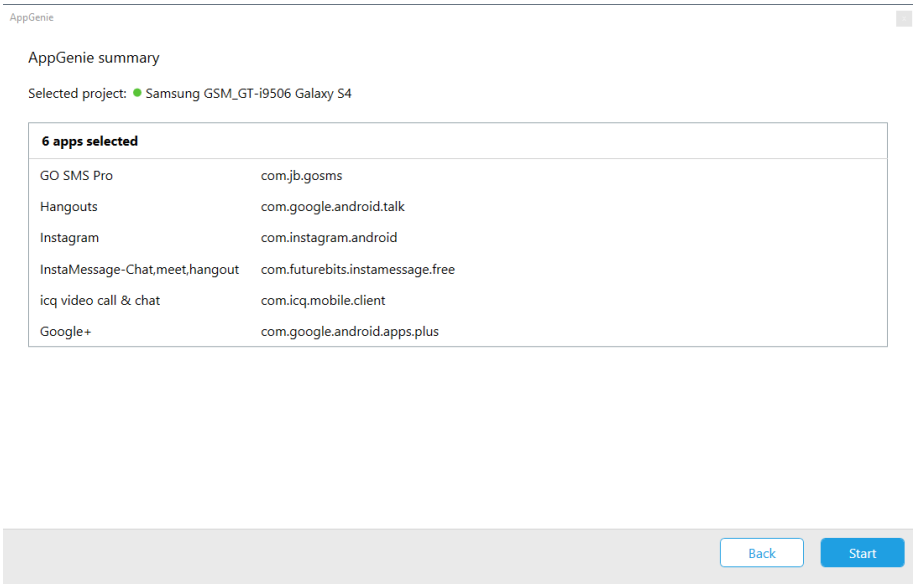
1. Select **Tools** > **AppGenie.** The following window appears.

2. Click **Next**. The following window appears.

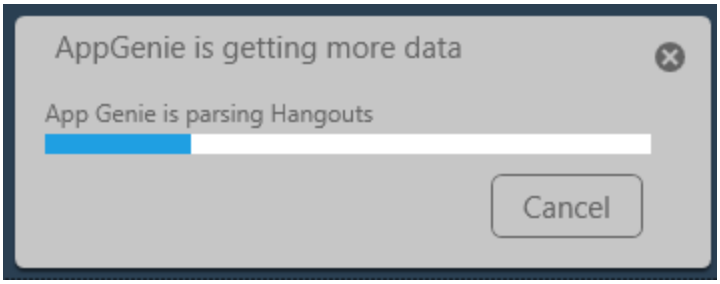


The actions and information displayed in this window are explained under App insights (on page 281).

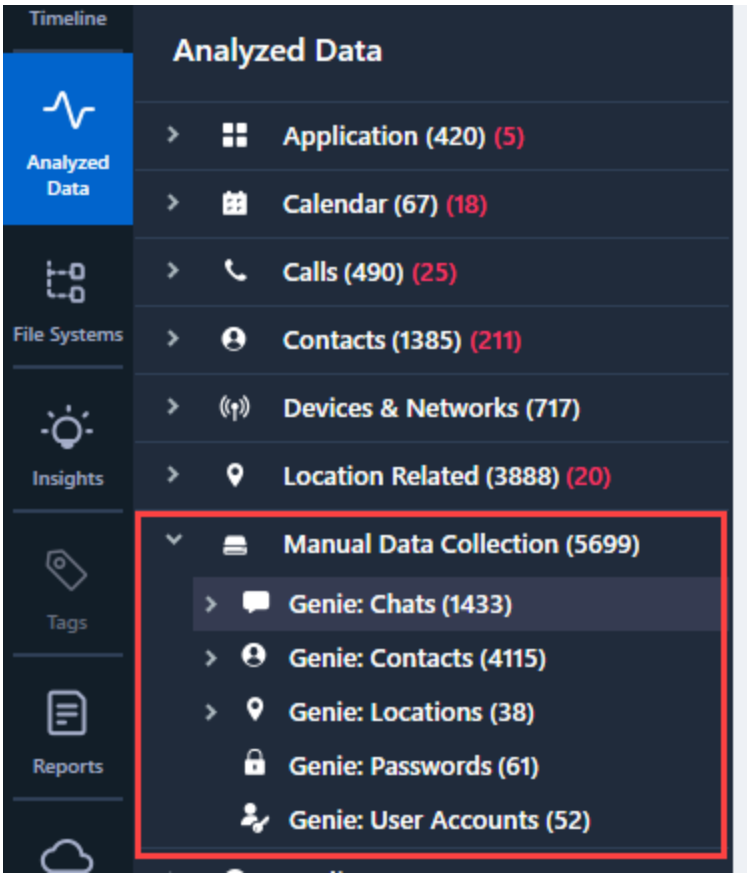
3. If you have more than one project open, select the Active project.
4. Select the Categories and apps from which you require additional data. You can search for the app, or add filters to refine the displayed apps by Emulatable apps or apps that were not decoded by Physical Analyzer.
5. Click **Open AppGenie** to access the Summary window. The following window appears.



6. Click **Start**. The following window appears.



The new artifacts are displayed in the Analyzed Data tree under **Manual data collection.**



11.3. Virtual Analyzer

The Virtual Analyzer enables you to view your data as if you were using the owner's device, validate decoded artifacts and recover data from unsupported apps. It requires an active Physical Analyzer license. The Virtual Analyzer is based on the Andy OS emulator, which is an external tool that simulates an Android device on your computer.

This emulator supports up to Android OS 7.0. The Virtual Analyzer tool complements other generic solutions such as SQLite and Fuzzy Models. To use the Virtual Analyzer, you need APK files, which are only extracted as part of Physical extractions (and some file system extractions).

To run the Virtual Analyzer:

You can now run the Virtual Analyzer in the following ways:

- Click the **Open Virtual Analyzer** button in the Extraction Summary.
- Right-click an app in the Installed Applications model and select **Open in Virtual Analyzer**.
- Select **Tools** > **Virtual Analyzer**.

> The **above options are not available** until an extraction with APK files is added to Physical Analyzer.

For more information, see the following topics:

Online/offline mode (on the facing page)

Virtual Analyzer notes (on page 290)

Installation process (on page 291)

Using the Virtual Analyzer (on page 294)

Emulation options (on page 299)

11.3.1. Online/offline mode

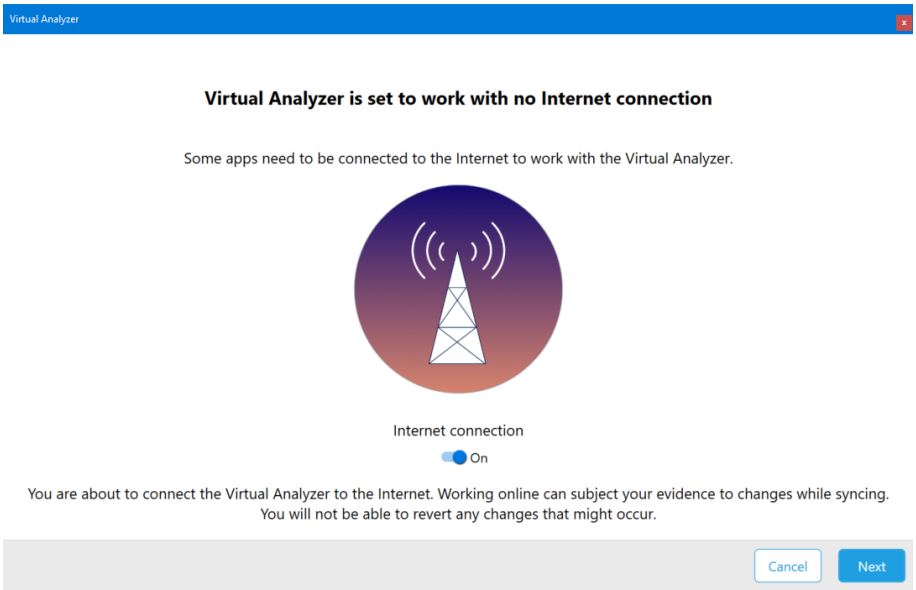
Apps which require Internet connection may not work properly or not have all the data. Running an app in the Virtual Analyzer is like running it in airplane mode. The default offline mode in Virtual Analyzer restricts Internet connectivity, so actions performed in the emulator are not synced with the app's servers.

> Working online can subject your evidence to changes while syncing. Additionally, you will not be able to revert any changes that may occur.

To switch to online mode:

1. Contact Cellebrite Support for the configuration file to enable online access.

   When selecting apps, the virtual Analyzer will now have the option to switch between online and offline mode.



2. Click the switch to On.

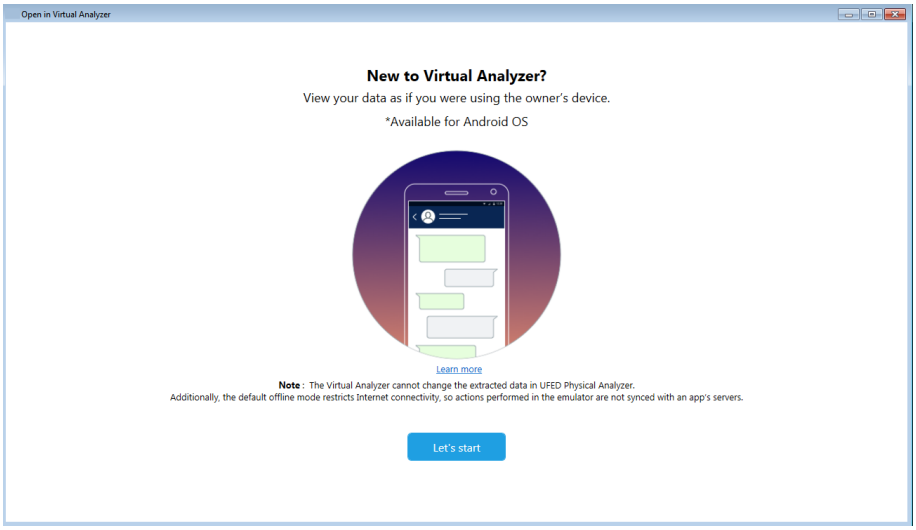
11.3.2. Virtual Analyzer notes

- The Virtual Analyzer installation may not complete successfully if graphics drivers are not fully updated. If you encounter installation errors, update your display drivers, restart your computer and try again.
- The Virtual Analyzer installation may not complete successfully if the VMware Player is already installed. If you encounter installation errors, uninstall the VMware Player and then try again.
- To install the Virtual Analyzer, VT-x must be enabled in your machine's BIOS. If you encounter errors during Andy OS installation, check that the VT-x is enabled in the BIOS. In every computer the steps for enabling it might be slightly different, but in general, in the BIOS settings you should look for are **Advanced > CPU Configuration** > **Intel Virtualization Technology (VT-x)** or something similar, change it to **Enabled** and click on **Save and exit**.
- The Virtual Analyzer is a generic Android solution, but currently does not support all apps.
- The Virtual Analyzer only displays the data as displayed by the device. Deleted files or metadata that are not displayed by the app, will not be displayed in the Virtual Analyzer.
- When running for the first time, or each time after closing the emulator window, the Virtual Analyzer performs a clean restart, and therefore takes longer to load (it's like restarting a mobile device).
- If the emulator window is open, you can load additional apps to the current session. The Virtual Analyzer window will be hidden until the new apps finish loading.
- To maintain data integrity, you cannot load APKs from different Physical Analyzer projects, into the same Virtual Analyzer session.
- UFDR files of physical extractions that include "Uncategorized" data files can also be used in the Virtual Analyzer, but not in Cellebrite Reader.
- The data in the Virtual Analyzer is writable (you can change the data presented in the Virtual Analyzer, such as delete a message from a chat, enter text etc.). The extraction itself will not be affected at any time. If the app will be re-opened in the Virtual Analyzer, your changes will not be saved. The Virtual Analyzer itself does not save the data, for each Virtual Analyzer session on a specific extraction, it will start from a clean slate.
- The Virtual Analyzer is a "virtualization" solution. Working on a virtual machine may cause it to work very slowly or not at all. We recommend working with Virtual Analyzer on a physical computer.
- Apps work the same way as if the device was in flight mode. App errors, pop-up windows, apps that are partially working, or not working at all could be due to no Internet connection.
- Stopping the emulation of an app in the middle might cause the Virtual Analyzer to restart and loaded apps will need to be re-loaded.

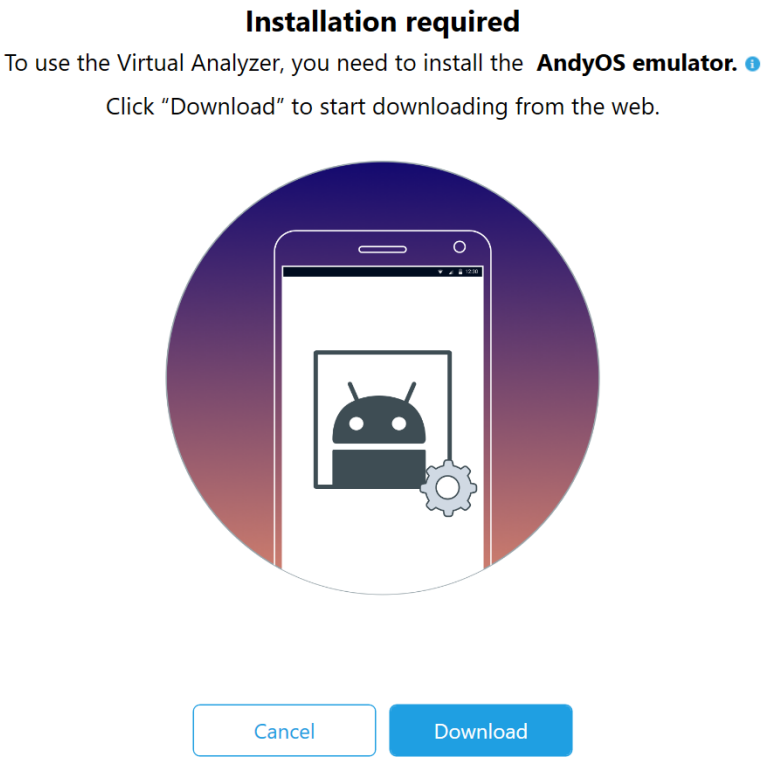
11.3.3. Installation process

To install the Virtual Analyzer:

1. Select **Tools** > **Virtual Analyzer**. The following window appears.



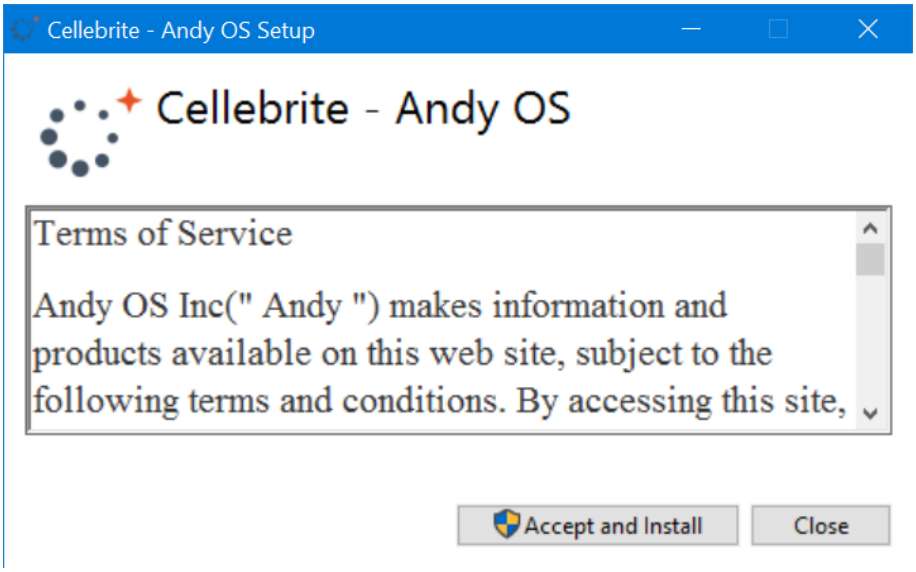
2. Click **Let's start**. The following window appears.



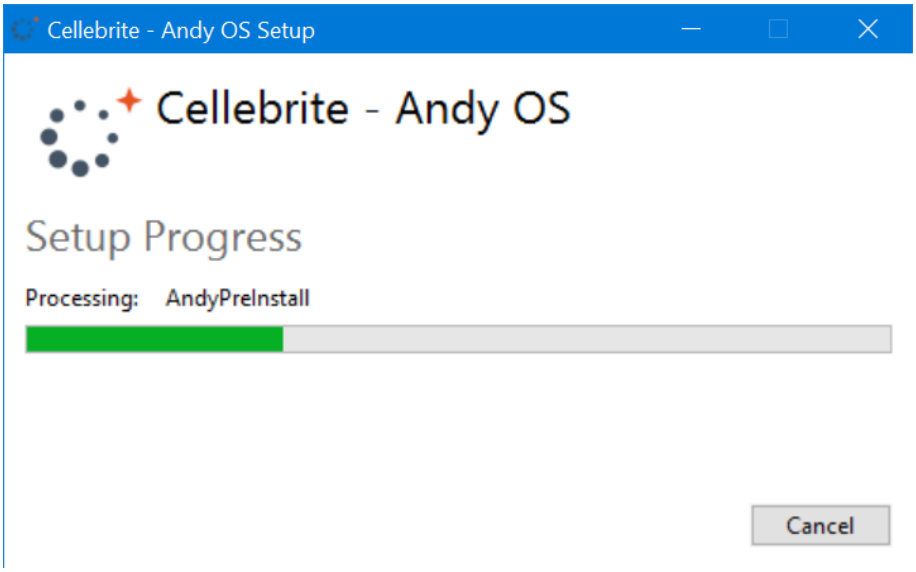
3. Click **Download** and wait for the file to download.

If you do not have Internet access, you can download the Virtual Analyzer from **MyCellebrite** > **Downloads**.

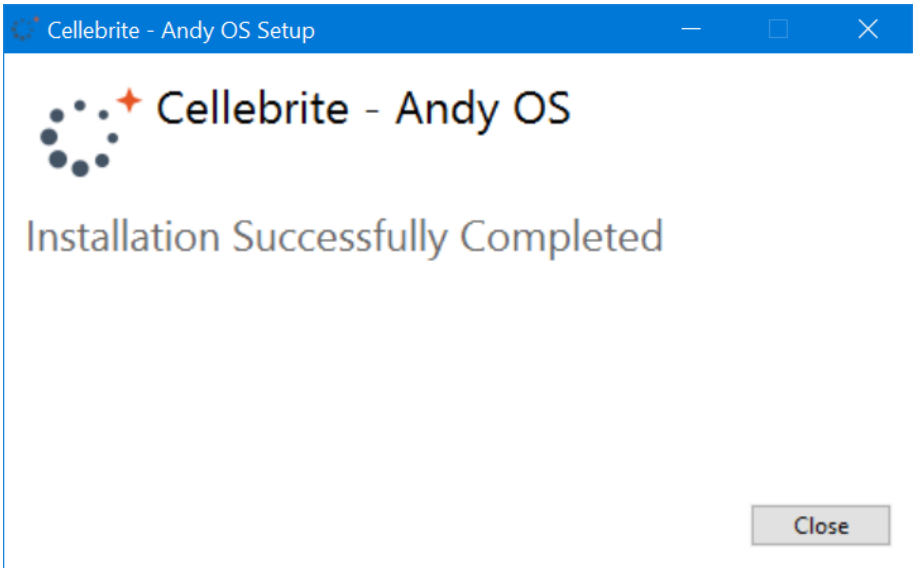
4. Unzip the `VirtualAnalyzerSetup.zip` file and then double-click the Andy setup file to start the installation process. The following window appears.



5. Click **Accept and Install**.
6. If required, click **Yes** to accept the Window account control warning to allow the app to make changes. The following window appears.



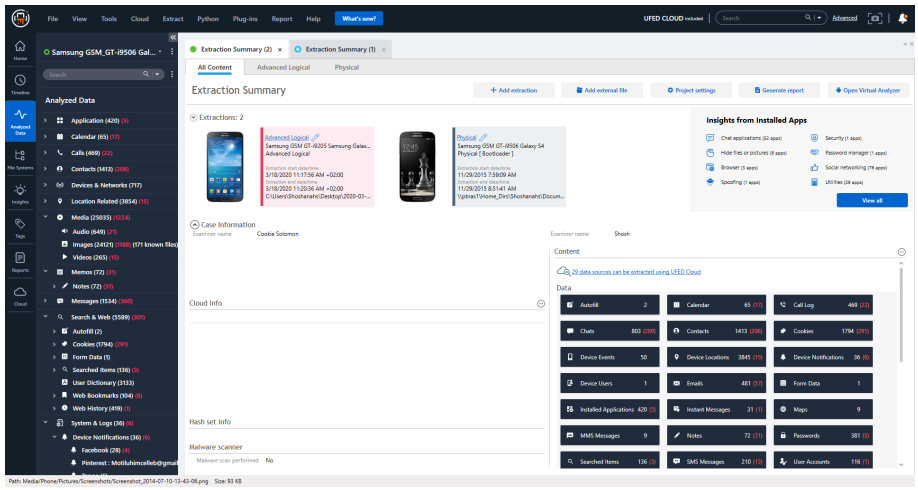
7. Follow and setup instructions and then wait for the setup process to finish. The following window appears.



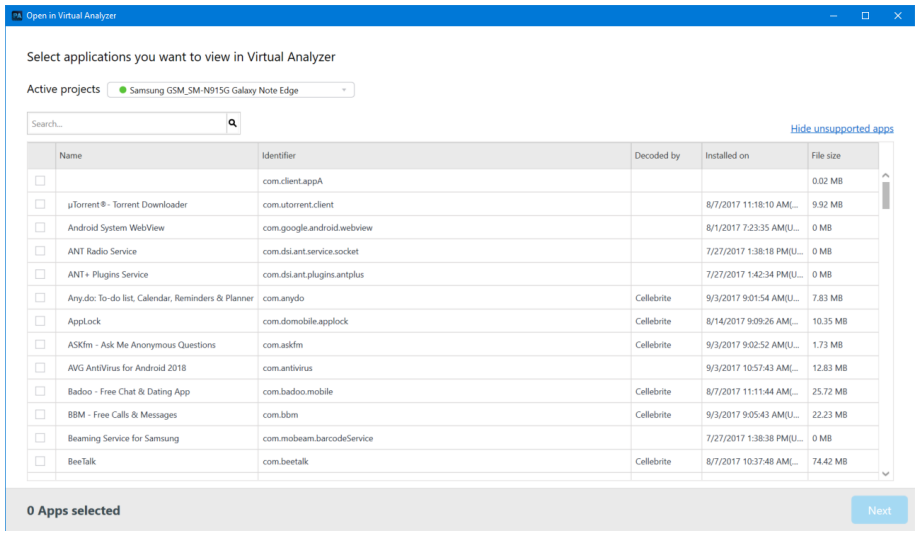
8. Click **Close**.

11.3.4. Using the Virtual Analyzer

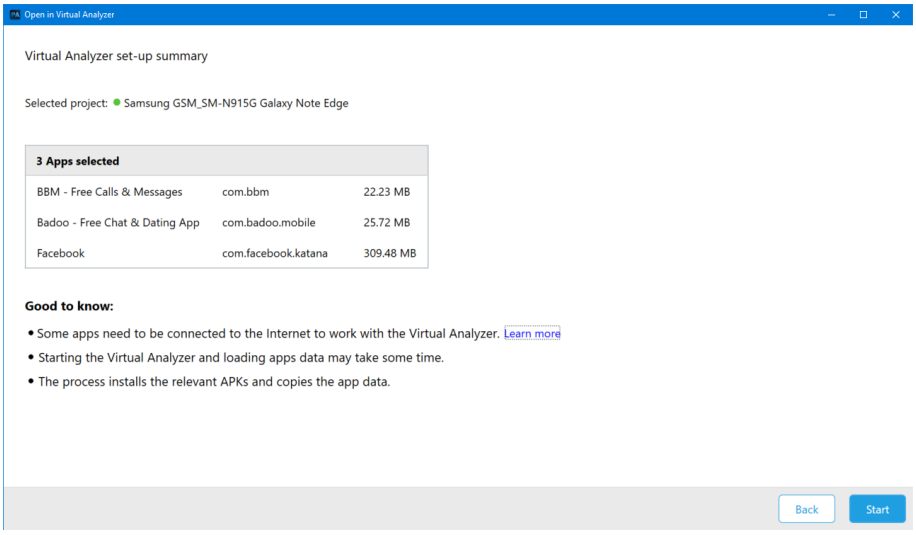
1. Use the Case wizard to add a physical extraction, then click **Start decoding**.



2. After the extraction finishes decoding, run the Virtual Analyzer. The following window appears.



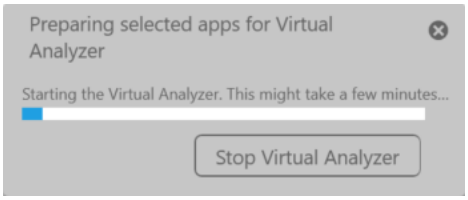
3. Click the **Hide unsupported apps** link to hide the apps that cannot be emulated.
4. Select the apps that you want to view in the Virtual Analyzer and then click **Next**. You can select a maximum of 5 apps. A message is displayed that the selected apps are being prepared for Virtual Analyzer and that the process takes time to complete. The following window appears.



This summary window explains what is going to happen in the following step. It displays the selected project, the selected apps and the size, and additional information.

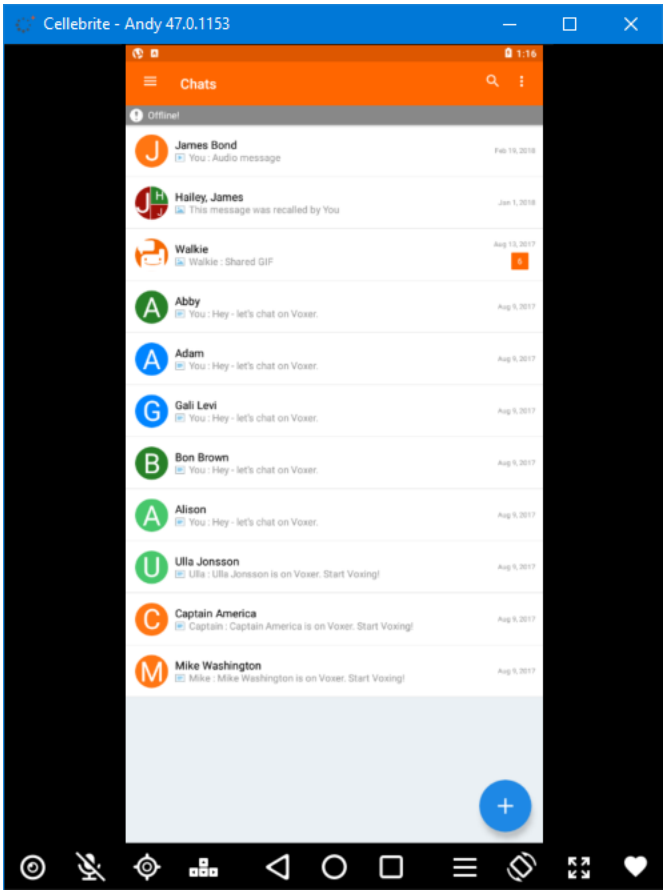
> The more apps you select the longer it will take to prepare the apps in the Virtual Analyzer.

5. Click **Start**. The following notification appears.

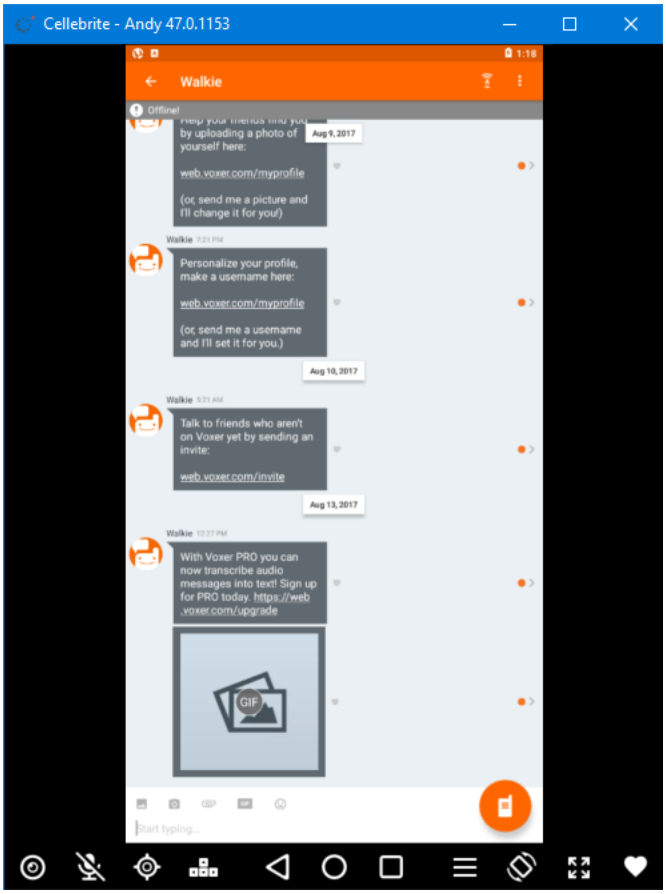


After a few minutes depending on the number and size of the apps the Virtual Analyzer appears.

6. Select the required app.



The following example shows a chat conversation for the selected app.



Use the Screen capture tool to capture images or videos of any relevant evidence and include them in the project. For more information, see Recording screen captures and video (on page 186).

11.3.5. Emulation options

The following information can be found in the Andy OS User Manual. For more information on using Andy OS, see the Andy OS User Manual.

Feature	Description
Camera	Pick the camera you want to use inside Andy. You can switch between cameras on-the-fly. You can also disable the camera entirely.
Microphone	Pick the microphone you want to use with Andy. You can also disable the microphone entirely.

Location	» Auto: Andy uses your system location if available. If not, your IP location will be used instead.
	» Manual: Andy uses the location you set manually in the GUI.
	  » Latitude: Adjusts latitude coordinates.
	  » Longitude: Adjusts longitude coordinates.
	  » Altitude: Adjusts the altitude.
	  » Accuracy: Adjusts how accurate the location reading is. This affects the blue circle around the indicator in Google Maps for example.
	  » Bearing: Adjusts the direction you are facing.
	  » Address: You can enter an address and hit Enter, this will take you to that address on the map.

Keymapper	Andy automatically picks the right keymapper configuration file for the running application from the designated folders. You can, however, manually choose a different configuration file at any time.
Menu	Not many applications use the menu button anymore. But for those old-school applications that do, you will be prepared.
Orientation	Andy switches its orientation intelligently based on the running application. If, however, you feel like changing the orientation manually, use this button.
Fullscreen	Andy enters the Fullscreen mode for a more immerse experience. The hotkey for this is F11. Or you can set Andy to start in Full screen.
Multitasking	To multitask in Andy and switch between running applications, simply press the square icon next to the home button (circle). This will open a window with all running applications which you can choose between. Pressing the home button while inside an application will not close it, but rather minimize it. To quit an application, you will need to access the multitasking menu then flick it off the screen. This will close the application completely and free up RAM and resources it was using.

11.4. Accessing public data

Publicly available data from social media channels has positively impacted investigations of all kinds, and has proved to be an excellent supplement. However, up until now many of the existing methods have been manual, time consuming and ineffective.

Physical Analyzer enables you to extract and preserve public domain, forensically sound data in one workflow. With an active Physical Analyzer license, you can enrich your extracted data sources, and quickly reveal evidence hiding in plain sight on Facebook, Instagram and Twitter.

To use this capability, you need to have an Internet connection available.

For more information, see the following topics:

Extracting the data (on the facing page)

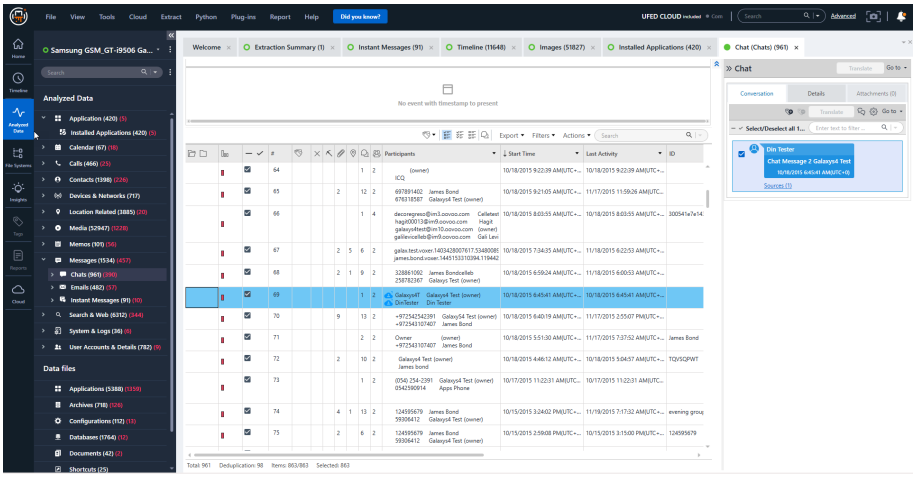
Creating a public domain avatar (on page 305)

Extracting public cloud account data (on page 234)

11.4.1. Extracting the data

You can extract a person's public data by providing an avatar[1]. Physical Analyzer will use it to log in to the data sources and extract public data about the person.

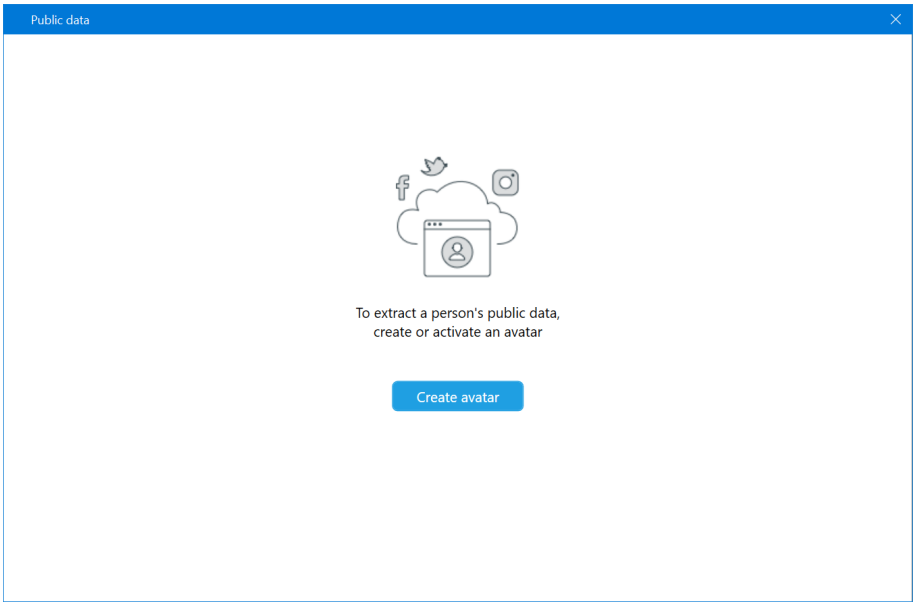
The data available for extraction is dependent on the relationship between the chosen avatar and the profile being extracted (for example, a friend of a friend may be able to extract more data than a stranger). Public data is available for the following models: Contacts, Call logs, Chats, Email, and Instant Messages. An example with public data is shown next.



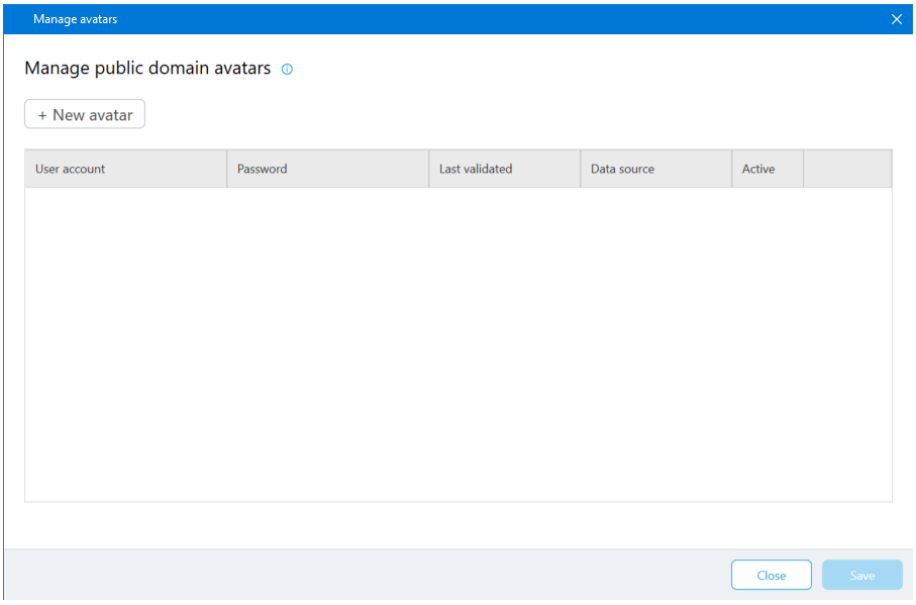
To extract public data:

1. Click the icon to see if there is more information on the person. The following window appears.

[1]A social media profile that you can use to extract public data. Note: Avatars are public profiles, and as such, are exposed to public review.

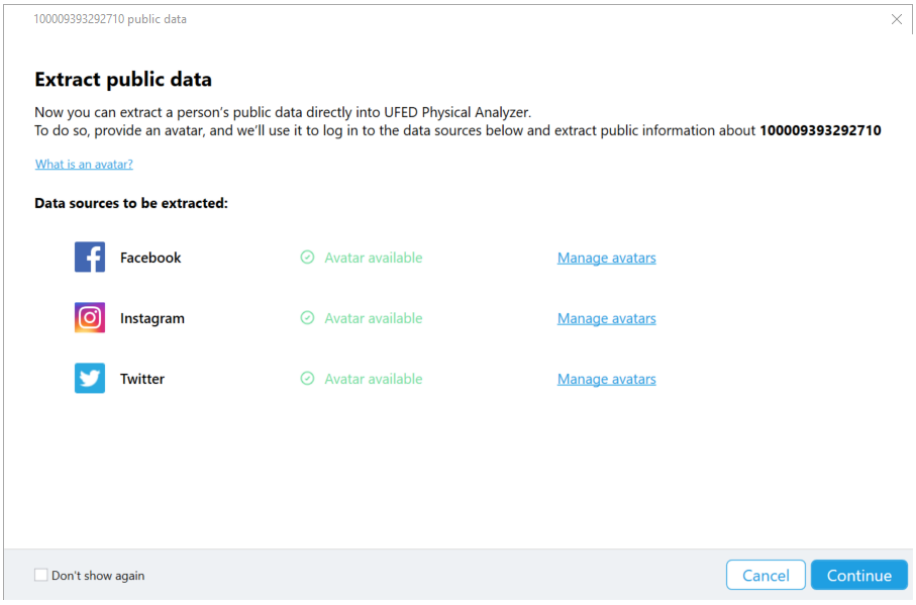


2. Click **Create avatar**. The following window appears.

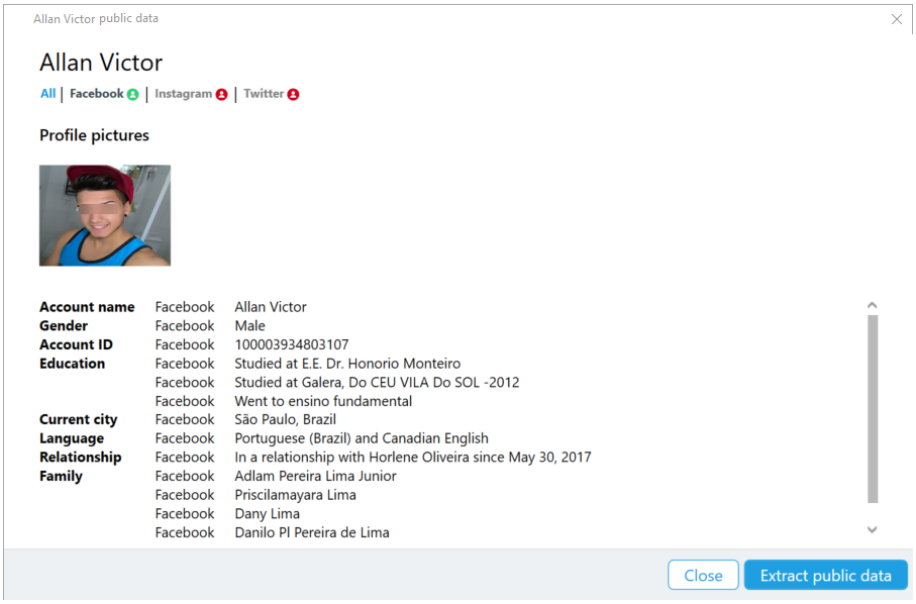


> If you have already created at least one avatar, you can skip this step.

3. Create the avatars. For more information, see Creating a public domain avatar (on page 305).



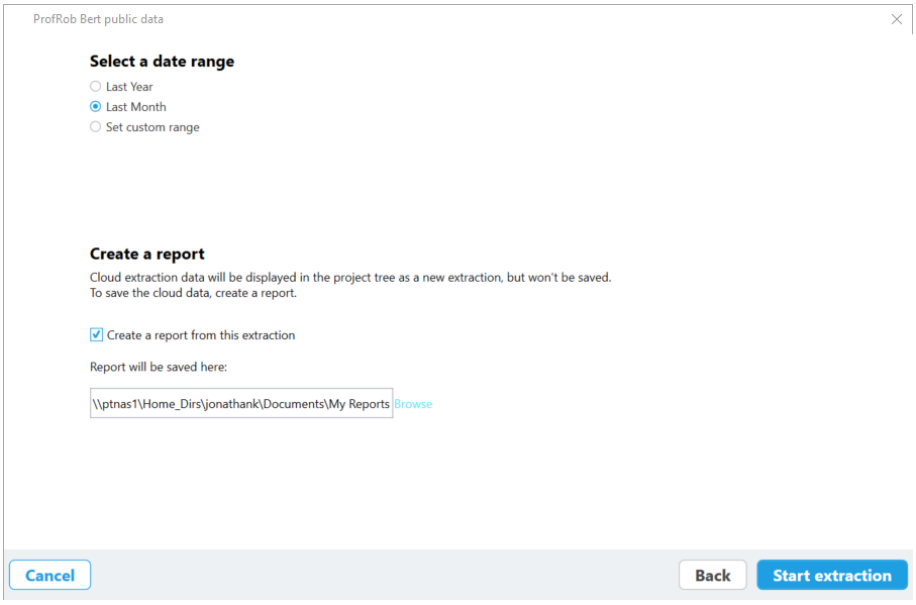
4. Click **Continue**. The following window appears.



This quick view shows the public details of the person and profile images, including account name, account ID, gender, education, age, occupation, relationship status etc.

> Public data may not be available for some people.

5. Click **Extract public data** to generate a full extraction of this person's public data. The following window appears.



6. Select a date range for extraction: Last year, Last month or set a custom range.
7. If required, select the **Create a report from this extraction** check box and specify the location of the report. The generated report is in UFDR format. The report includes all the extracted public data for this person so data will not be lost when you close the application. Once the extraction is complete you can view the data as a new separate project.

> The extracted public data will be displayed in the project tree as a new extraction, but the data will not be saved. To save the public data, you need to create a report.

8. Click **Start extraction**.

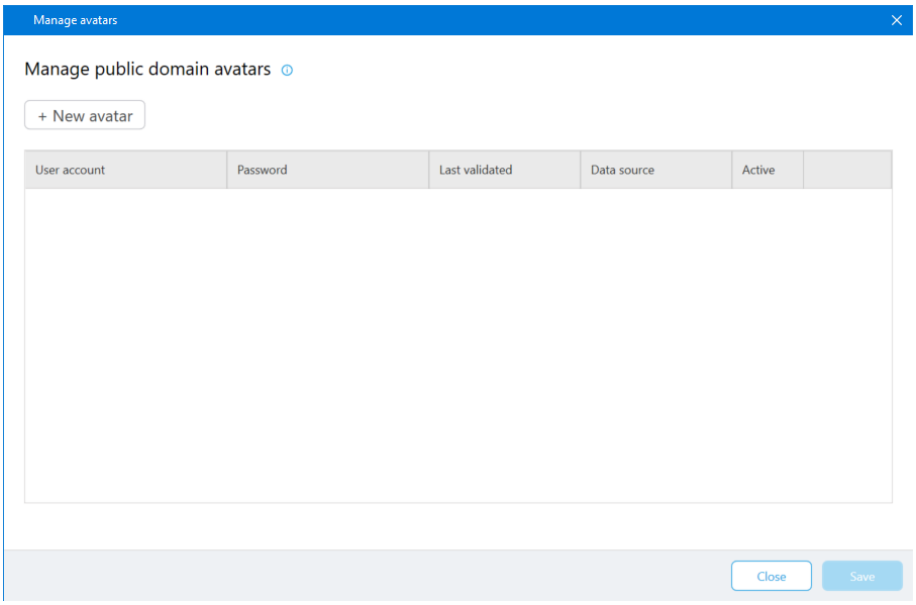
11.4.2. Creating a public domain avatar

An avatar[1] is a social media profile that you can use to extract public data. It's not recommended to use a private account. When selecting an avatar, keep in mind that it's exposed to public data view.

> To prevent the Twitter account from being locked, it's recommended to add a mobile number to the source account.

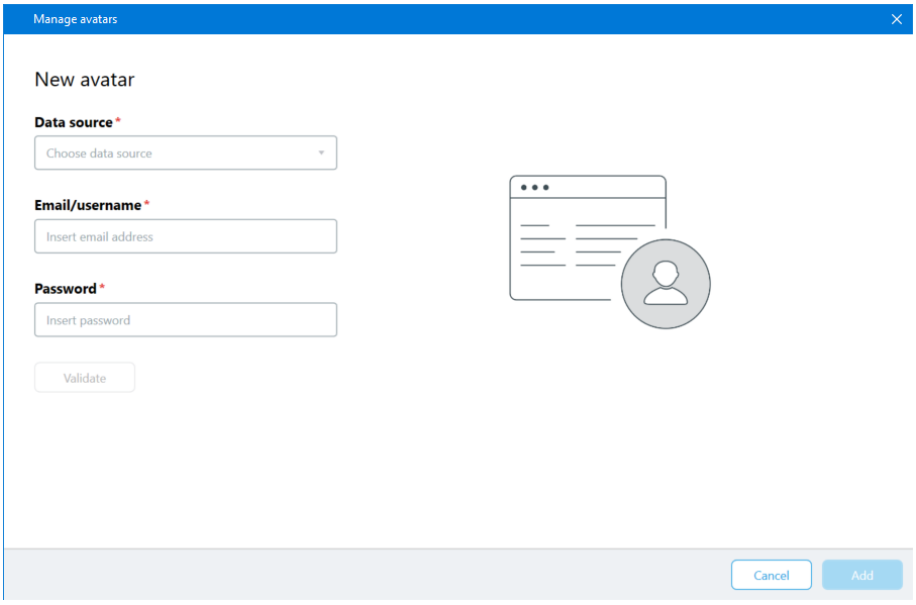
To create an avatar:

1. From the **Tools** menu select **Manage public domain avatars.** The following window appears.

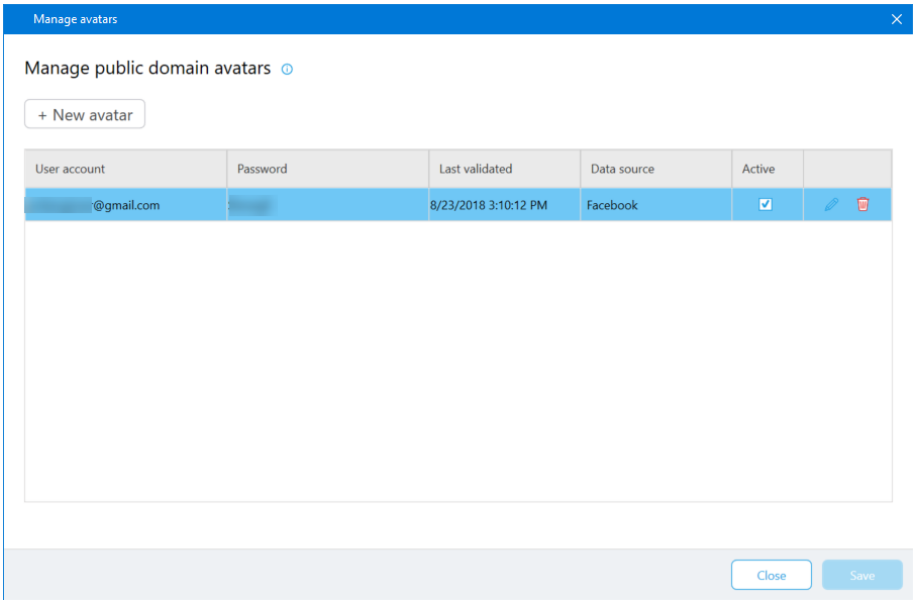


2. Click **New avatar**. The following window appears.

[1]A social media profile that you can use to extract public data. Note: Avatars are public profiles, and as such, are exposed to public review.



3. Select the data source: Facebook, Instagram or Twitter.
4. Enter the email or username.
5. Enter the password.
6. Click **Validate**. A message is displayed that the avatar was validated successfully.
7. Click **Add** to add the avatar. The following window appears.



From this window, you can add additional avatars, activate or deactivate an avatar, edit the credentials for the avatar or delete an avatar.

11.5. SQLite wizard

With the SQLite wizard you can visually decode additional data from databases, particularly from unfamiliar databases that were not decoded and may contain important case information. This tool enables you to build queries and map database fields to Physical Analyzer models. Generated reports indicate fields that were manually decoded using this tool.

All queries are managed in the SQLite query manager, where you can select to auto-run the query as part of the automatic decoding process, and save a query for future use.

> Encrypted content and attachments are not yet supported.

> This tool is for a single database only.

To use the tool, you need to perform the following steps:

- Identifying a database (on the next page)
- Building the query (on page 311)
- Mapping data (on page 321)
- Running the created query (on page 327)

Enhance your forensic skills and learn more about SQLite database structures with the following recommended training course:

Cellebrite Advanced Smartphone Analysis (CASA)

4-day, Expert-level Certification

Participants will learn to:

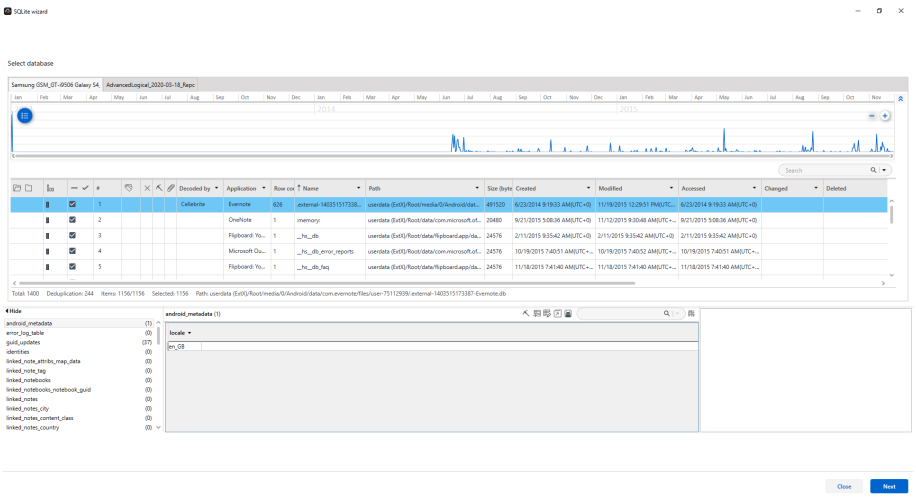
- Conduct in-depth examination, forensic recovery of application data in SQLite databases
- Use techniques to defeat passcodes
- Analyze user data and system artifacts in iOS and Android devices using Physical Analyzer and third-party tools.
- Create reports using physical analyzers / SQLite Wizard

11.5.1. Identifying a database

Select a database from the list of databases under Data Files. You can also access the SQLite wizard from the **Tools** menu or button. In Databases view, you can see whether the databases were decoded by Physical Analyzer, manually decoded by the SQLite wizard or not decoded at all. We recommend that you select a database that has not yet been decoded.

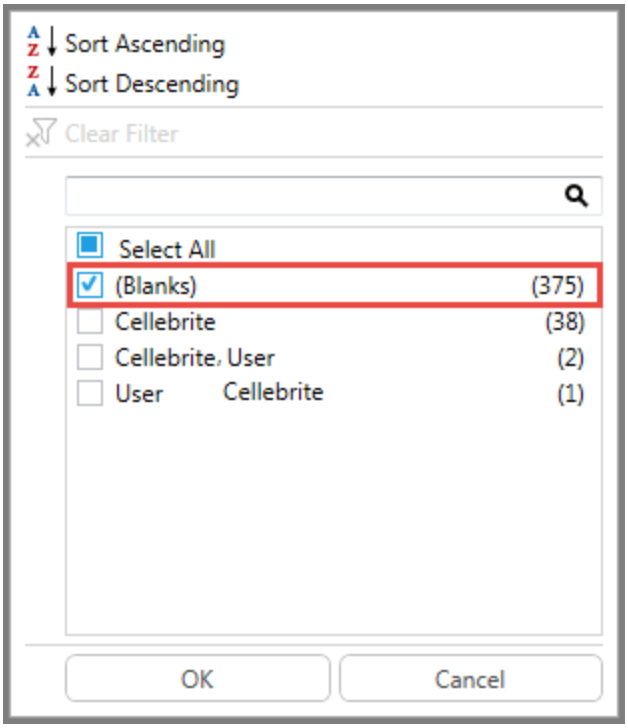
To select a database that was not decoded:

1. In Analyzed data tree under **Data Files** select **Databases**, or click **Tools** > **SQLite wizard** > **Select database**. The Database tab or Select database window appears.



> Only SQLite databases are displayed in the Databases window.

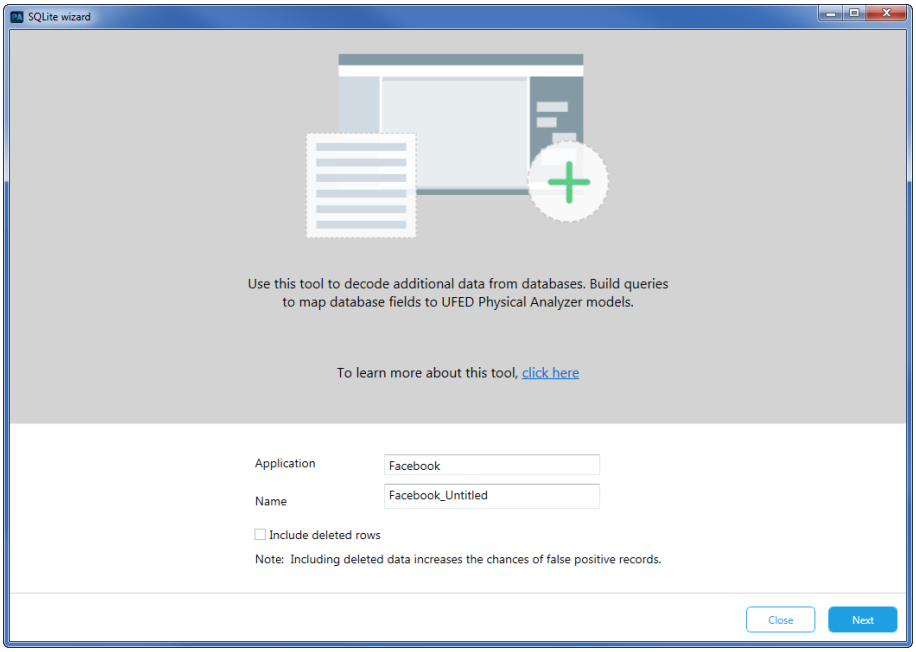
2. In the Decoded by column, select the **(Blanks)** check box so that only databases that are not decoded are displayed. An example is displayed next:



The options in this window are as follows:

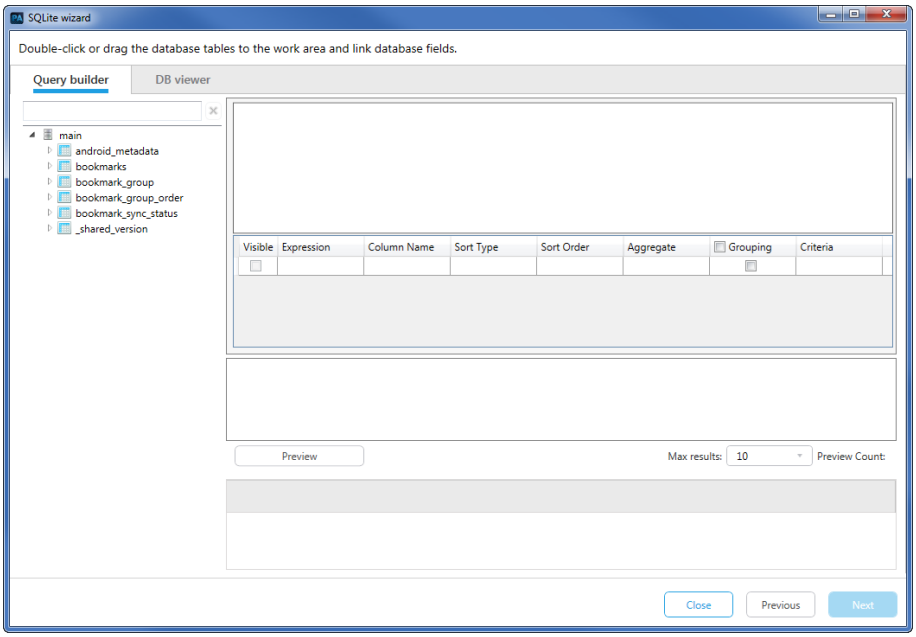
Select All	Select all databases.
(Blanks)	Select only databases that were not decoded.
Cellebrite	Select only databases that were decoded by Physical Analyzer.
Cellebrite, User	Select only databases that were decoded by Physical Analyzer or manually decoded.
User	Select only databases that were manually decoded.

3. Select the required database, right-click and then select **Open in SQLite wizard** . The SQLite wizard starts and the following window appears:



The application name is displayed only if the application can be identified by the system. This field can be edited.

4. Enter a name for the query.
5. Select the **Include deleted rows** check box, if you want to include deleted data. Including deleted data increases the chances of false positive records.
6. Click **Next**. The following window appears.



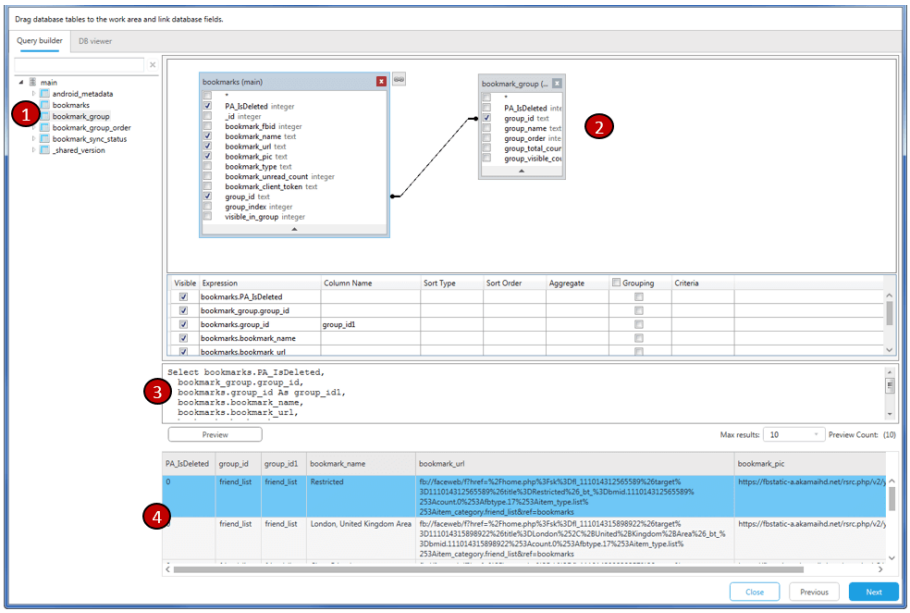
11.5.2. Building the query

After identifying the database, drag the database tables to the work area, and create relationships between tables that will automatically generate a SQLite query. Alternatively, you can write your own SQLite query. You can then preview the results.

> Advanced options can be used for renaming, sorting, linking and grouping capabilities. See Advanced options (on page 318).

To build the query:

1. Click the **DB viewer** tab to review the databases and fields.
2. Double-click or drag the database tables to the work area.



1 Database tables area

2 Work area

3 SQLite query area

4 Preview area

> In the Max results list, you can select the maximum number of results to be displayed in the Preview area of the window, or you can the default value (10 results).

3. If required, you can link (join) fields from different tables. This is useful if you need to combine records from two tables with matching values in a field common to both tables. Other actions, such as adding a derived table, adding common table expressions, using unions and setting properties, are also available.

   > You can also edit or enter SQLite queries in the space provided.

4. Click **Preview** to preview the results.

   > Make sure that the selected query is correct before you click **Next**. The query cannot be edited in the following steps.

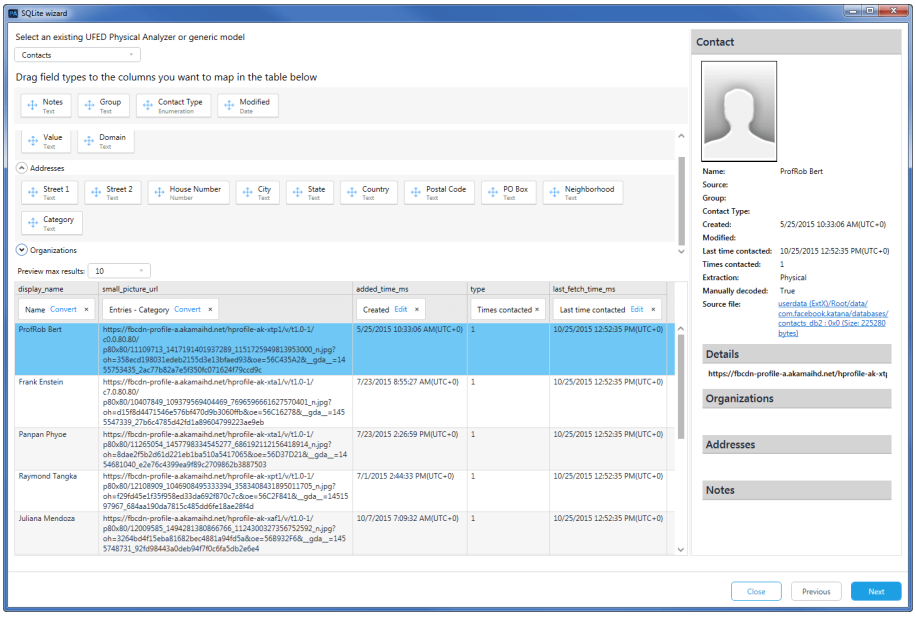
5. Click **Next**. To help you map the relevant fields and columns, the results are simulated in the right pane view.

   For examples of the model types and field descriptions, see Model types and descriptions (on the facing page).

11.5.2.1. Model types and descriptions

The following examples show some of the model types as well as explanations of the fields in these models.

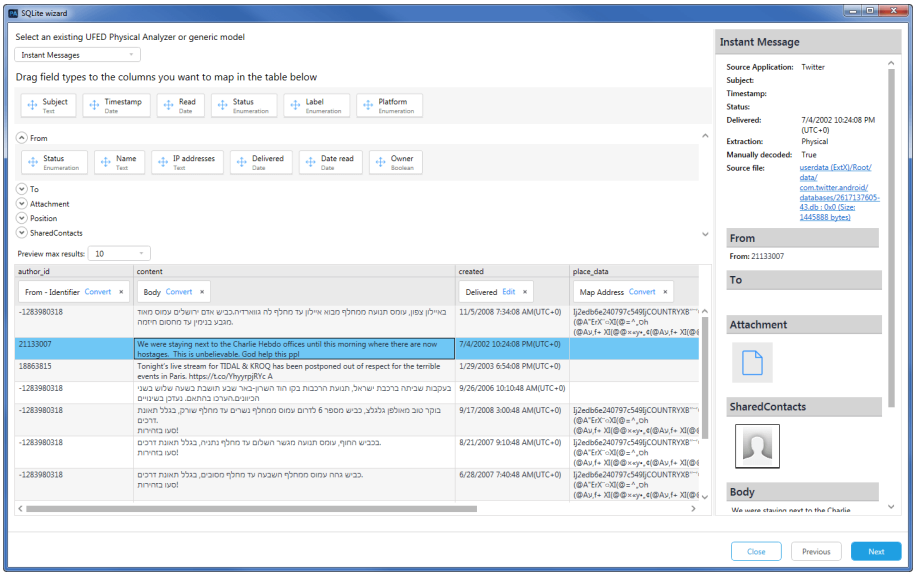
11.5.2.1.1. Contacts



Field	Type	Description
Name	Text	Name of the contact. If the Name field is left blank, the entry is not listed in the address book of the device.
Notes	Text	Additional user-created notes added to the user's contact entry.
Group	Text	Refers to a group's contact details that can be stored on the device.
Contact Type	Enumeration	The type of contact. E.g., Unknown, Follower, Following, FollowingAndFollower, Spam, Blocked, Starred, PendingRequest, Favorite, Suggested, Group, and ChatParticipant.
Last time contacted	Date	Date and timestamp converted from UTC (Universal Time Coordinated).
Created	Date	A stored log on the device of when the contact was created.
Modified	Date	A stored log on the device of when the contact was modified.
Times contacted	Number	A stored log on the device for the number of times contacted.

Field	Type	Description
Entries		
Category	Text	Any category information e.g., Fax, Work, Email, URL
Value	Text	Value for the Category.
Addresses		
Street1	Text	Location or address information of the contact entry.
Street2	Text	
House Number	Number	
City	Text	
State	Text	
Country	Text	
Postal Code	Text	
PO Box	Text	
Neighborhood	Text	
Category	Text	
Organizations		
Name	Text	Name of the organization or business.
Position	Text	The contact's position or title.

11.5.2.1.2. Instant Messages

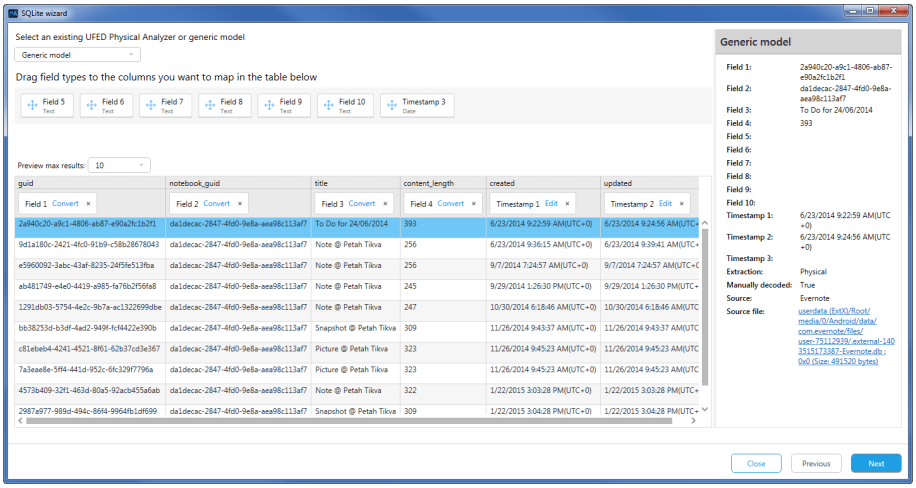


Field	Type	Description
Subject	Text	The user created subject line of an entry. Applicable for social media chats that describe a name or subject of a group.
Body	Text	The body of the message.
Timestamp	Date	A network timestamp which may be recovered for a message.
Read	Date	Date the message was read.
Delivered	Date	Date the message was received.
Map Address	Text	The street address, city, and state associated with the message.
Status	Enumeration	Status of the message as marked in the device (Sent, Unsent, Read, Unknown).
Label	Enumeration	The label applied to the message (Default, Star, Liked, Disliked).
Platform	Enumeration	The platform used for the message (Unknown, PC, Mobile).
Message Type	Enumeration	Differentiates between the different types of Messages: App message, SMS, MMS etc.
SMSC	Text	For SMS messages, the short message service center (SMSC) that handled the message.

Field	Type	Description
Folder	Text	The folder that contains the message.
Priority	Enumeration	The priority of the message.
From		
Identifier	Text	The unique ID for the party. e.g., email address, GUID, nickname etc.
Status	Enumeration	Status of the message as marked in the device (Sent, Unsent, Read, Unknown)
Name	Text	Name of the party.
IP addresses	Text	IP address of the device.
Delivered	Date	Date the SMS was received.
Date read	Date	Date the message was read.
To		
Identifier	Text	The unique ID for the party. e.g., email address, GUID, nickname etc.
Status	Enumeration	Status of the message as marked in the device (Sent, Unsent, Read, Unknown).
Name	Text	Name of the party.
IP addresses	Text	IP address of the device.
Delivered	Date	Date the message was received.
Date read	Date	Date the message was read.
Attachment		
Filename	Text	The name of the attachment.
Contact type	Text	The type of contact. Unknown, Follower, Following, FollowingAndFollower, Spam, Blocked, Starred, PendingRequest, Favorite, Suggested, Group, and ChatParticipant.
Charset	Text	Character set encoding.
URL	Text	A URL string associated with the attachment.
Title	Text	Title text for the attachment.

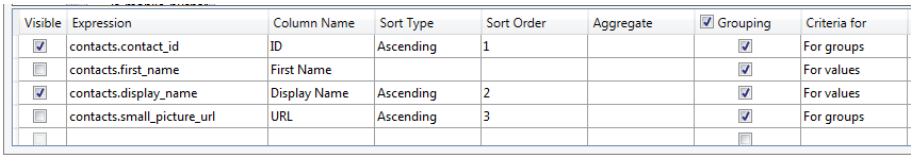
Field	Type	Description
Position		
Longitude	Number	Coordinate of the message in longitude.
Latitude	Number	Coordinate of the message in latitude.
Elevation	Number	Elevation data.
Comment	Text	Any comment text added to the location.
Shared Contacts		
Name	Text	Name of the contact that was sent.
Notes	Text	Any notes added to the sent contact.
Group	Text	Group information (if the contact was sent to a group).
Contact type	Enumeration	The type of contact. Unknown, Follower, Following, FollowingAndFollower, Spam, Blocked, Starred, PendingRequest, Favorite, Suggested, Group, and ChatParticipant.
Created	Date	A stored log on the device of when the contact was created.
Modified	Date	A stored log on the device of when the contact was modified.
Times contacted	Number	A stored log on the device for the number of times contacted.

11.5.2.1.3. Generic model



11.5.2.2. Advanced options

Advanced options include renaming, sorting, linking, and grouping capabilities.

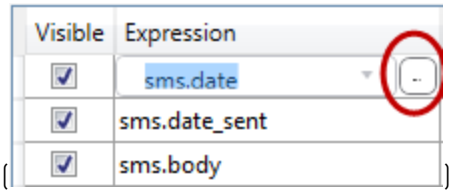


Visible	Expression	Column Name	Sort Type	Sort Order	Aggregate	Grouping	Criteria for
☑	contacts.contact_id	ID	Ascending	1		☑	For groups
☐	contacts.first_name	First Name				☑	For values
☑	contacts.display_name	Display Name	Ascending	2		☑	For values
☐	contacts.small_picture_url	URL	Ascending	3		☑	For groups
☐						☐	

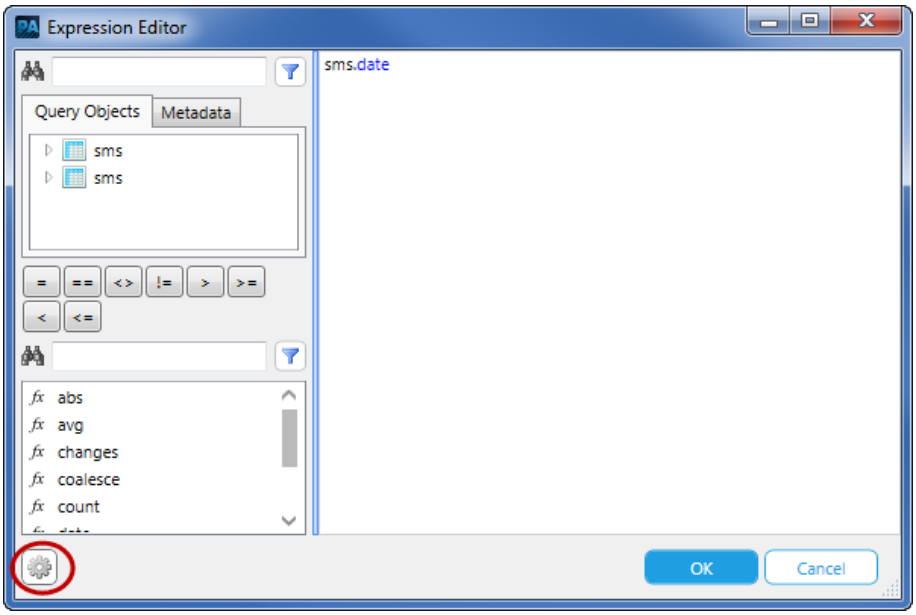
The following advanced options are available:

Option	Description
Visible	Select whether the field is displayed or not.
Expression	Select the field to display or click the **Expression** button.
Column Name	Enter a name for the column.
Sort Type	Select a sort type: Descending or Ascending.
Sort Order	Enter the sort order for the field.
Aggregate	Select an aggregation option.
Grouping	Select if this field should be grouped.
Criteria for	Select a criterion: values or groups.

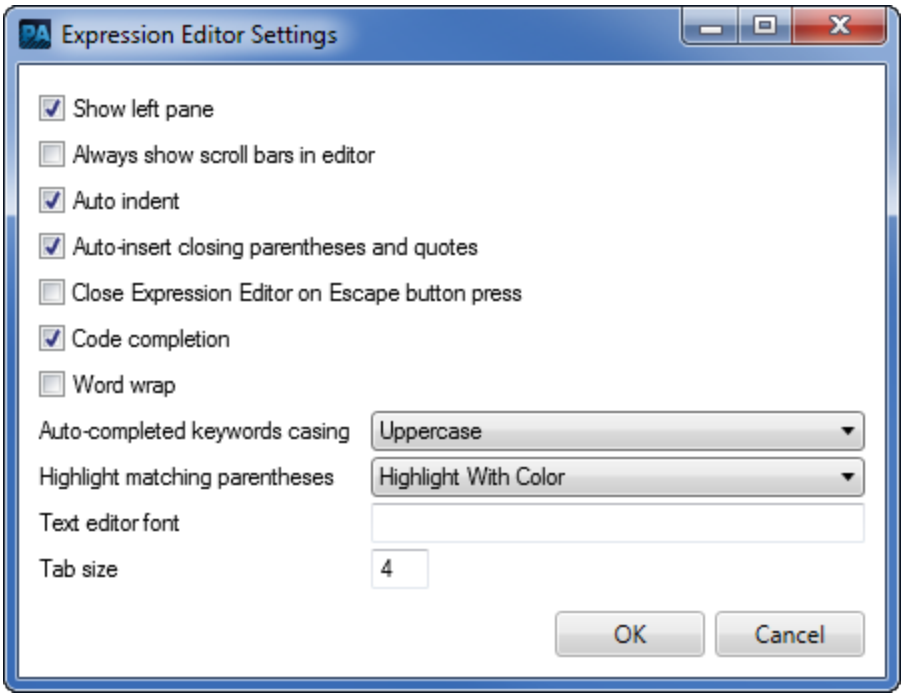
To open the Expression Editor:

1. Click the button next to the Expression (

), and then select **Expression Editor**. The following window appears.



2. Click the **Settings** button ( ) to change the Expression Editor Settings.



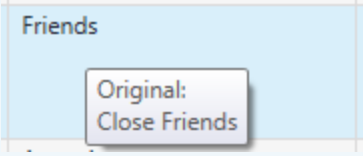
3. Make the required changes.
4. Click OK.

11.5.3. Mapping data

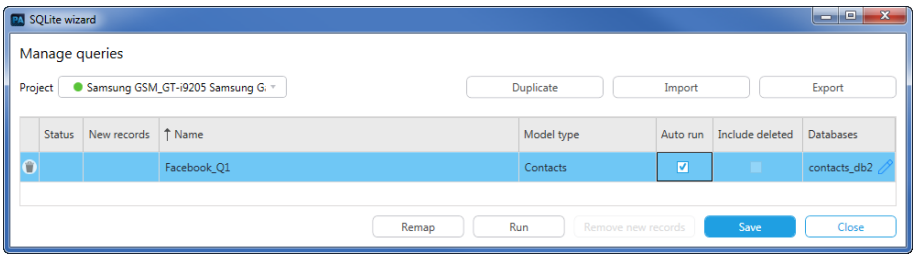
Select one of the existing data models (e.g., Chats, Contacts, Call logs, Instant messages etc.) or a generic model, and drag the field types to the correct columns. Some columns have special formatting options (see SQLite option windows (on the next page)).

To map the data:

1. Select an existing Physical Analyzer or generic model. If the fields match an existing Physical Analyzer model, then you should use that model. New records that are found by the SQLite script will be included in the selected model under Analyzed Data. If you cannot find a matching model use the default generic model. The Generic model is indicated as a separate model under Analyzed Data.
2. Drag the field types to the correct columns. You can drag more than one field type to a column to map multiple fields. Click **Edit** to edit the mapping. Click **Convert** to map new values. Some columns have special formatting options, enabling you to convert enum, lookup, XML/PLIST/JSON, and timestamp formats (see SQLite option windows (on the next page)).

> In the Preview area, mouse over the fields to see the original value of the field. An example is displayed next.
>
> 
>

3. Click **Next**. The following window appears.

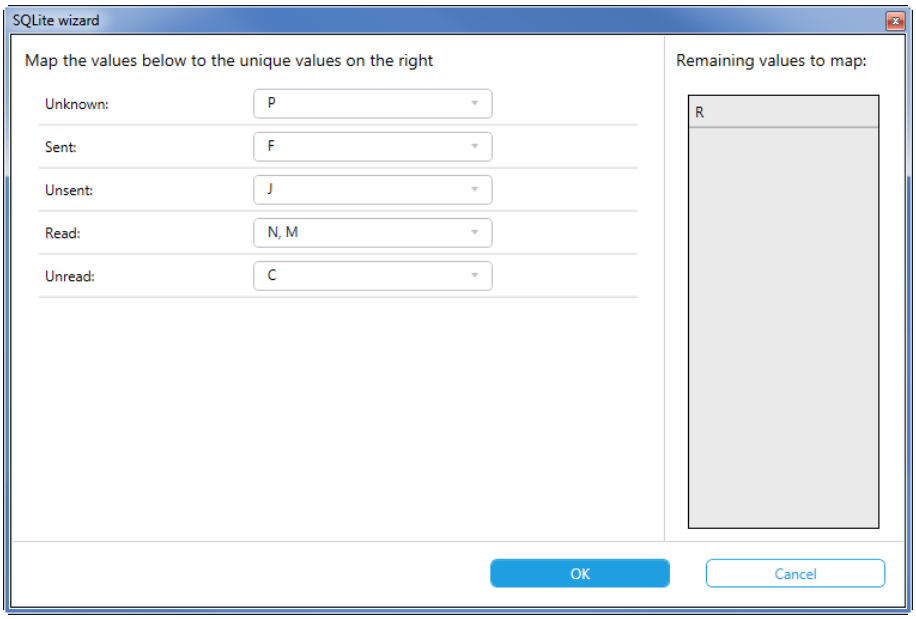


11.5.3.1. SQLite option windows

Some models have columns with special formatting options, enabling you to convert enum, lookup, timestamp and XML/PLIST/JSON formats and help you map the relevant fields and columns.

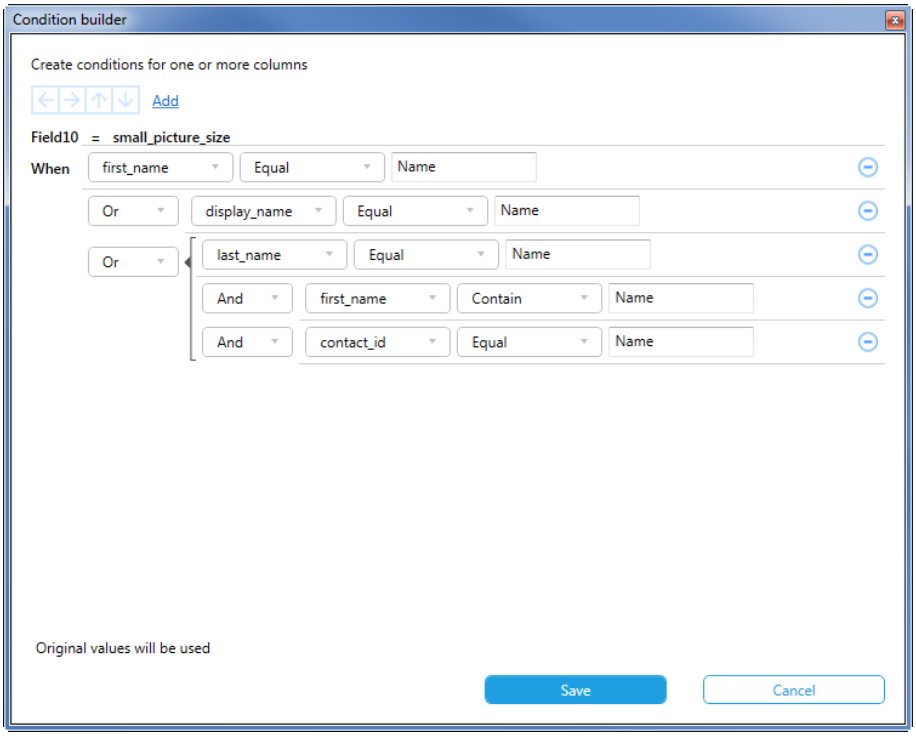
11.5.3.1.1. Enum

Select the values to map to the unique values on the right. An example is shown next.



11.5.3.1.2. Conditions

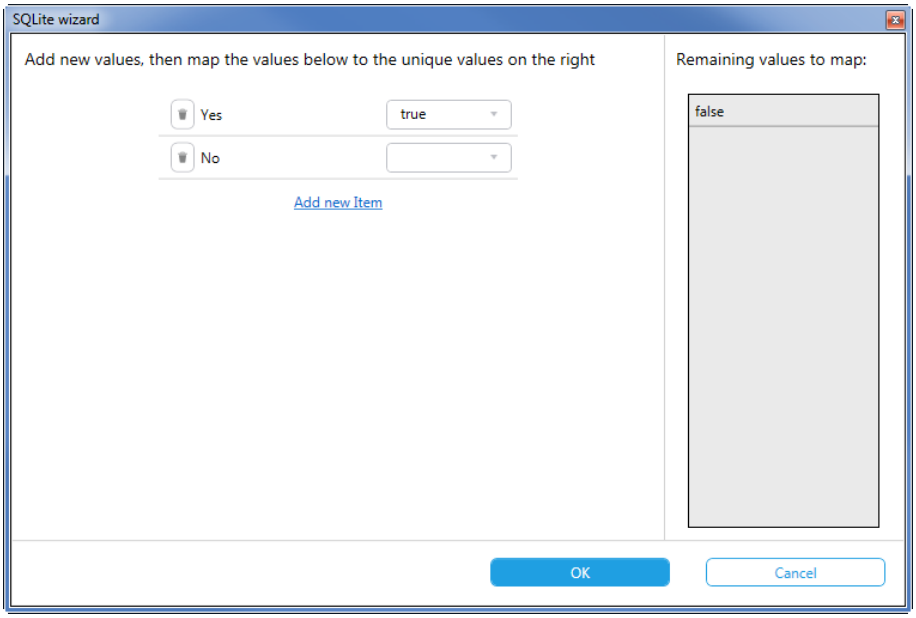
In cases where the interpretation of a field is based on another field's value, you can map that data using the conditions function. For example, an SMS participants table in an SQLite database contains SMS information. In several cases, the same column will contain both From and To values for the SMS message. You can create a new condition to distinguish between the two different field values. An example is shown next.



Use the **Add** link to add additional conditions with an "or" between them by default. Use the selection arrows to move the conditions. Moving a condition to the right will create a group with an "and" relationship between the conditions. Click **Save** to save the condition.

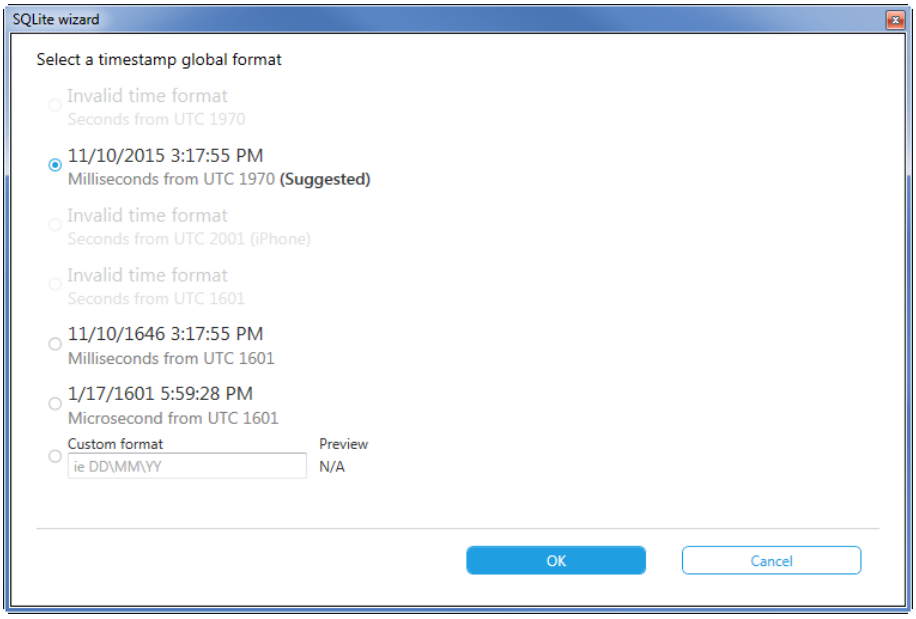
11.5.3.1.3. Lookup

Use a lookup window to add new values which can then be mapped to the unique values on the right. The number of look up records is partial i.e., it may not include all records. You can manually add additional values if required.



11.5.3.1.4. Timestamp

Use the suggested timestamp global format or select one of the other available options. You can also manually add additional options. An example is shown next.

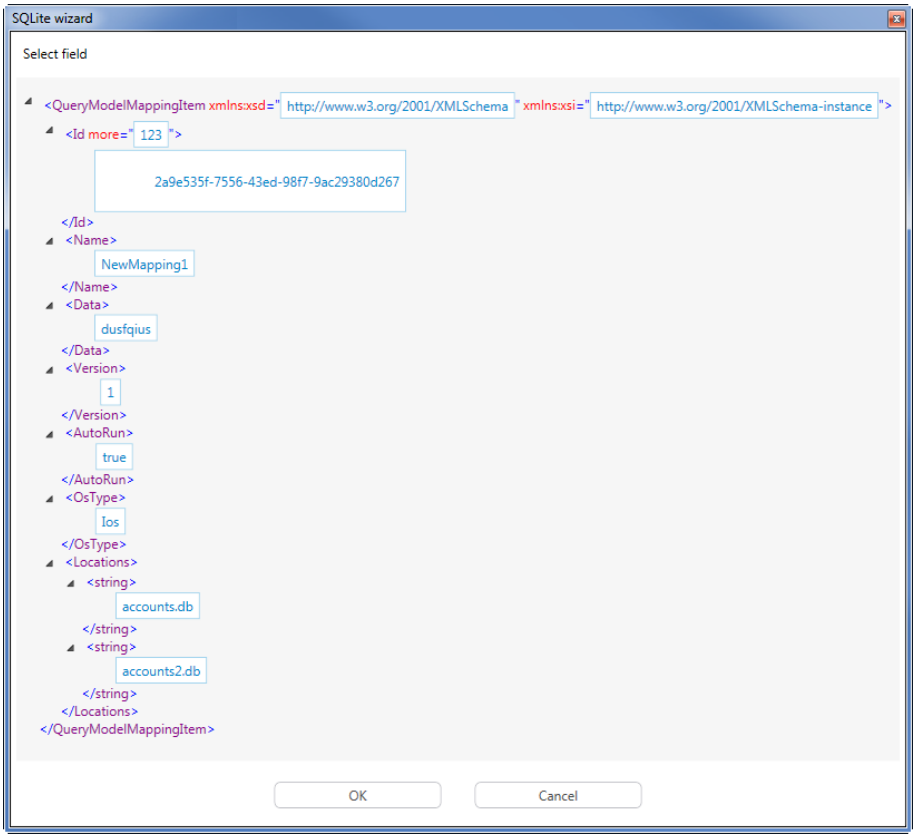


The Custom format can be used for timestamps that are in text format. Enter the required format and click OK. Some custom format examples are displayed next.

Custom format examples	Preview
M-d-yy h:mm tt	02-14-19 9:19:00 AM
M/d/yyyy h:mm tt	5/1/2009 6:32 PM
M/d/yyyy h:mm:ss	2019/07/12 08:22:48 PM
MM/dd/yyyy hh:mm:ss	5/1/2009 6:32:00

11.5.3.1.5. XML/PLIST/JSON

If a field includes XML, PLIST or JSON, the following window appears after you drag a field to the required column. Select the fields to map and click OK. After mapping the field, click the **Edit** link to make additional changes, click **Converter** to map new values, or click the **Preview** button ( ) to preview the code. An example is shown next.



Fields with a blue border indicate that the fields can be mapped.

11.5.4. Running the created query

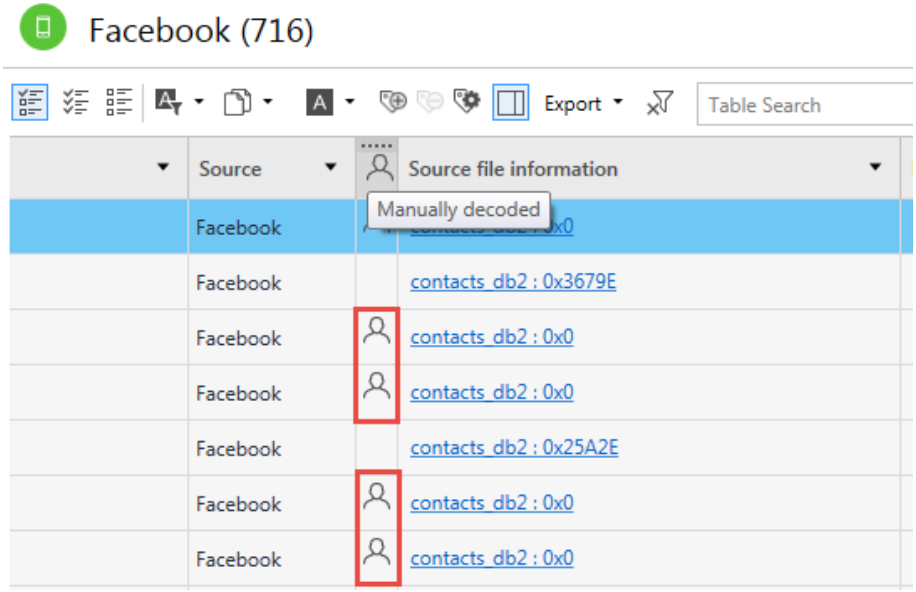
New records added by means of a manual query are indicated in the Manage queries window. For information on how to manage queries, see Managing queries (on the next page).

To manually run a query:

1. Select the project (if you have more than one project open).
2. In the table, select the required query that you want to run.
3. Click **Run**.
4. A message appears asking you to confirm that you want to run the mapping. Click **Yes**.

> Running a query with more than 200,000 results will significantly increase the processing time and may cause the system to stop responding.

5. New records are indicated under the model in the **Manually decoded** column. An example is displayed next.



11.5.5. Managing queries

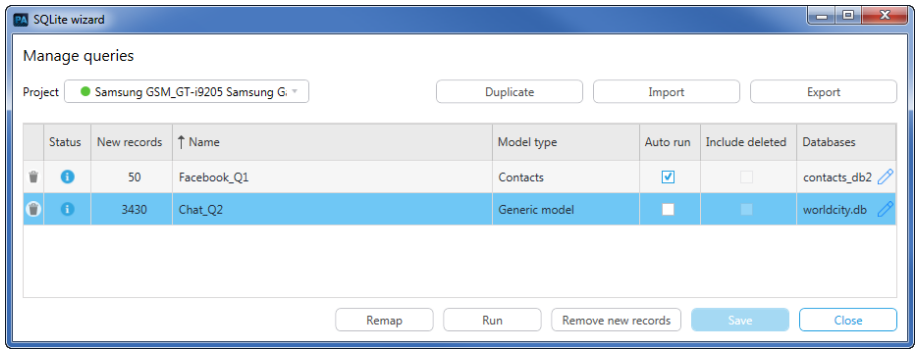
All queries are managed in the SQLite query manager, where you can select to auto-run the query as part of the automatic decoding process (see Running queries automatically (on the facing page)) and save a query for future use.

With the SQLite query manager, you can also:

- Add, edit and delete queries.
- Run queries on demand and remove records if required.
- View the number of new records per query.
- Share the queries with colleagues using the Export and Import features.

To open the SQLite query manager:

- Click **Tools** > **Database query builder** > **Open SQLite query manager**. The following window appears.



The following table explains all the actions and options available in this window:

Option	Type	Description
Auto run	Check box	Set Physical Analyzer to run the query automatically.
Databases	Column	Display the name of the database.
Delete	Button	Delete queries.
Duplicate	Button	Duplicate an existing query.
Edit	Button	Edit or add additional names for a database.
Export	Button	Export a query, which can then be imported and used by other users.
Import	Button	Import a query that was created by another user.

Option	Type	Description
Include deleted	Column	Display if this query includes deleted data. This option is read-only and cannot be changed.
Model type	Column	Display the Physical Analyzer model type.
Name	Column	Display the name of the SQLite query.
New records	Column	Display the number of new records that were found after running a query. "No results" indicates that the database is not found or there are no records in the database.
Project	menu	Select the project on which the query should be run (If you have more than one open project).
Remap	Button	Remap or change the query.
Remove new records	Button	Remove (rollback) the new records that were found after running the query.
Run	Button	Run a selected query.
Save	Button	Save any changes that were made.

Running queries automatically

You can select to auto-run a query as part of automatic decoding process.

To run a query automatically:

1. Select the **Auto run** check box.
2. If required, modify the database location using the **Edit** button.
3. Click **Save**.

11.6. Fuzzy models

The Fuzzy model plugin enables you to add valuable data from new databases. It identifies new data sources, handles and parses unknown databases and numerous applications databases. Information is automatically analyzed using a heuristic process and a unique set of rules. The Fuzzy model plugin is useful when the use of an application is known and has not been automatically parsed.

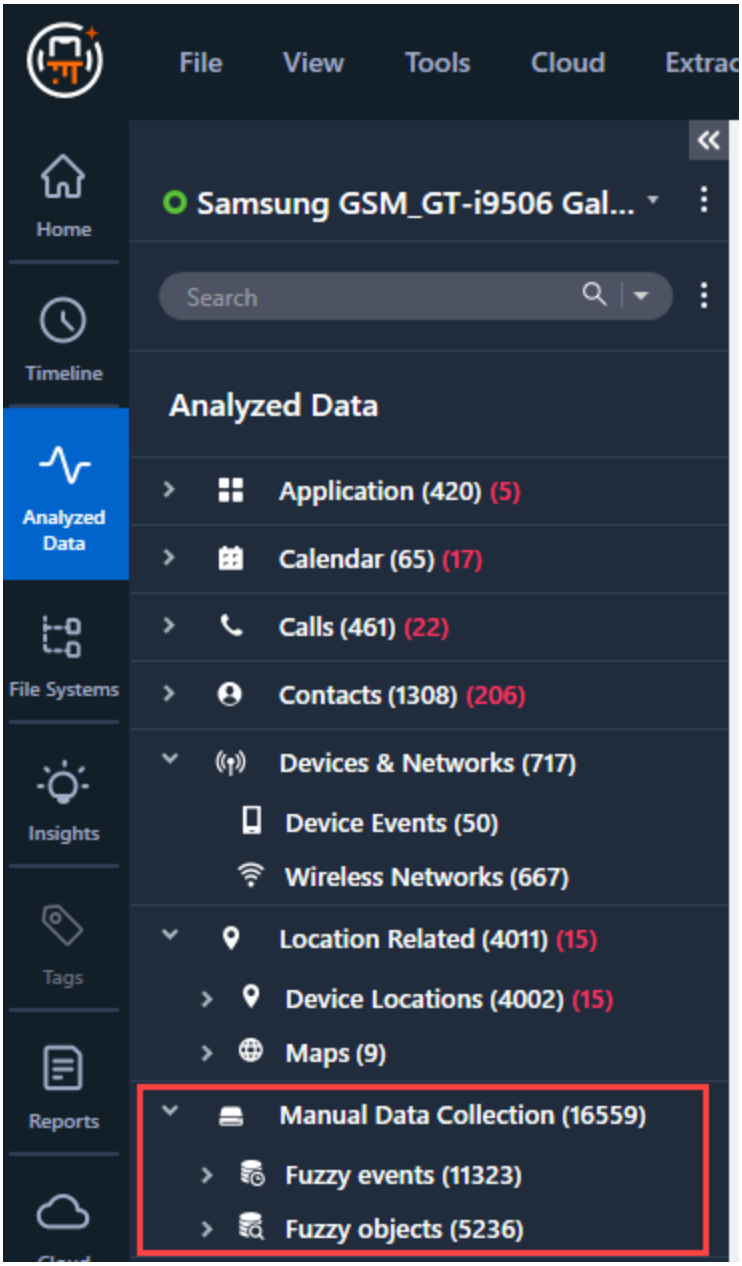
The Fuzzy model plugin scans and analyzes all databases and all tables within the databases, and automatically maps the records into a known models (e.g., email, IM, events, call logs etc.).

The following fuzzy models are available:

- **Fuzzy events:** View extracted events such as messages, call logs etc.
- **Fuzzy objects:** View extracted data from any database which has not decoded by Physical Analyzer's parsers. This model holds information regarding a certain artifact such as contact, account etc.

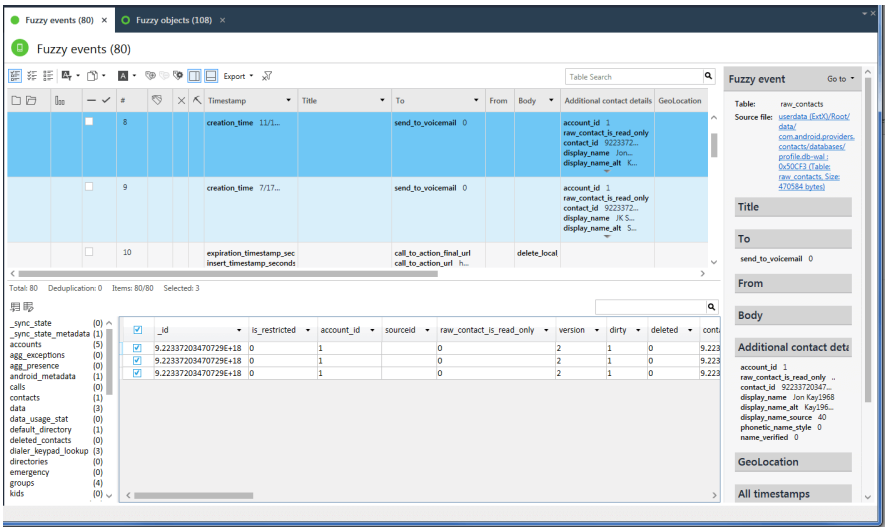
To run the Fuzzy model plugin:

1. Wait for the decoding process to complete.
2. Select **Tools** > **Run Fuzzy model plugin.** This will be initiated on the active project only. The Fuzzy models are indicated as separate models under Analyzed Data.



3. Open both the Fuzzy events and Fuzzy objects models, and review the parsing results. For each of these models, you can see the list of results presented in a table and database format, which displays the contents of database files that were found in the extraction. An

example is displayed next.

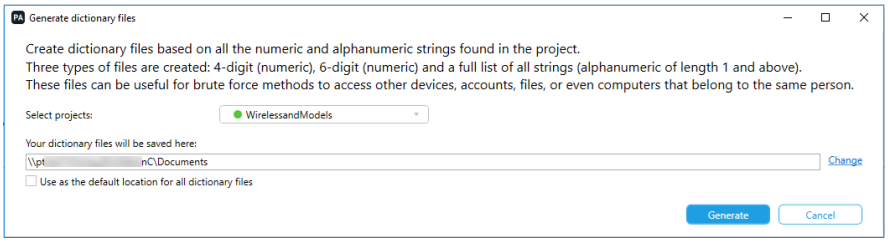


11.7. Generating dictionary files

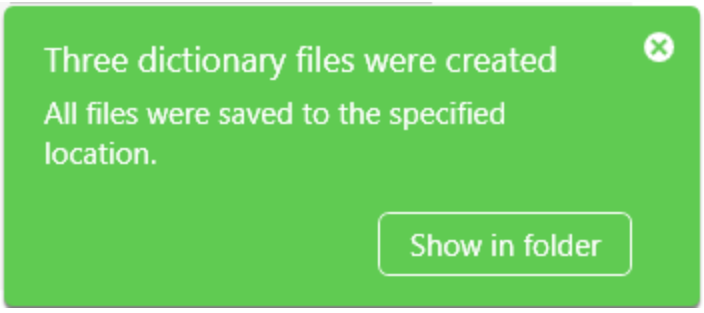
Create dictionary files based on all the numeric and alphanumeric strings found in the project. Three types of files are created: 4-digit (numeric), 6-digit (numeric) and a full list of all strings (alphanumeric of length 1 and above). These files can be useful for bruteforce methods to access other devices, accounts, files, or even computers that belong to the same person.

To generate the word lists:

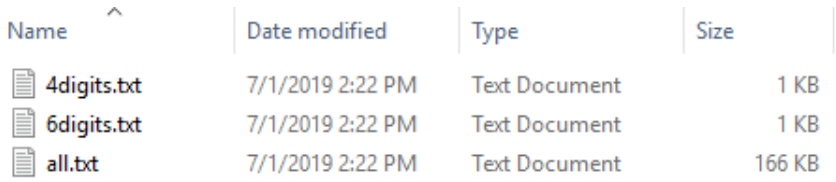
1. Select **Tools** > **Generate dictionary files**. The following window appears.



2. Select the required project.
3. Click **Change** to change the default location where the text files will be saved.
4. Select the **Use as default location for all dictionary files** to change the default location. The default location is specified under **Settings** > **General Settings**. See General settings (on page 421).
5. Click **Generate**. The dictionaries are created and the following notification is displayed.



6. Click **Show in folder** in the notification to access the word lists. An example is displayed next.



Name	Date modified	Type	Size
4digits.txt	7/1/2019 2:22 PM	Text Document	1 KB
6digits.txt	7/1/2019 2:22 PM	Text Document	1 KB
all.txt	7/1/2019 2:22 PM	Text Document	166 KB

11.8. Working with TomTom

TomTom generates trip log files that are encrypted by the device only if TomTom users select to share their location information with TomTom. TomTom registers the device location in the trip log files. Export the TomTom XML file generated from the trip logs, and send it to Cellebrite for processing. Once returned, you can view most of the location information available in the file using Physical Analyzer.

For more information on extracting data from a TomTom device, see Reading data from a GPS or mass storage device (on page 278).

For more information on geolocations, see Device locations (on page 170).

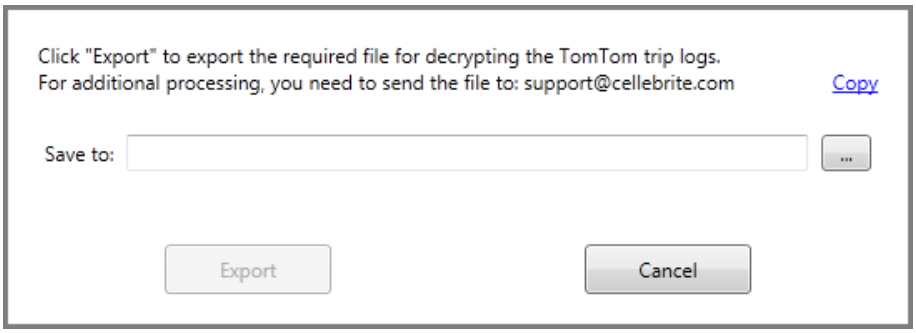
> Not all the information contained in the TomTom extraction file is retrievable.

> The processing service can take up to a few days, depending on the volume of data and requests. The service is currently free of charge, but this may be subject to change.

> You must open the TomTom extraction in Physical Analyzer before exporting or importing the XML file.

11.8.1. Exporting a TomTom file

1. Open an extraction from a TomTom device.
2. In the **Tools** menu, select **TomTom** > **Export**.



3. Browse to the location where you want to save the exported TomTom extraction file, and click **Save**.

   The TomTom extraction file is saved as a GPS.TomTomExport.xml file.

> The file does not contain personal user information such as locations.

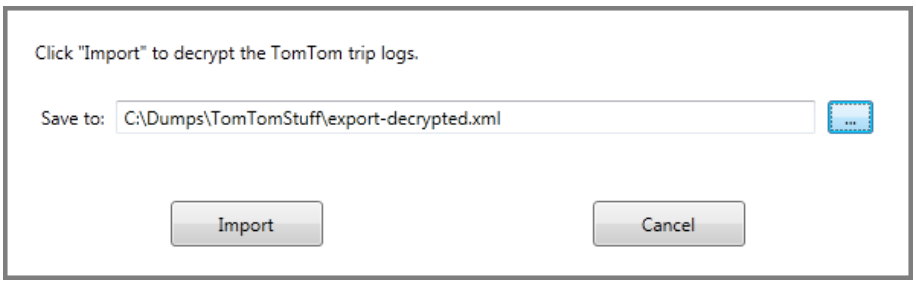
4. Send the GPS.TomTomExport.xml file to: support@cellebrite.com. For US customers: support@cellebriteusa.com.

   The GPS.TomTomExport.xml file is processed by Cellebrite support. Your request enters a queue at Cellebrite support. Processing of the TomTom extraction file may take a few days.

11.8.2. Importing a TomTom file

Once Cellebrite support has returned your processed TomTom XML file, import the file to Physical Analyzer.

1. Open the TomTom extraction for which you have the *.xml file.
2. In the **Tools** menu, select **TomTom** > **Import**.



3. Click ... and browse to the location of the returned TomTom extraction *.xml file, and click **Open**.
4. Click **Import**.

   The TomTom *.xml file is imported to Physical Analyzer. The **Locations** tree item is populated.

5. Double-click **Locations** to open the tree item in a data tab.

   The tab shows the device's location at every three seconds with a time and date stamp and geographical coordinates.

> Not all the information contained in the TomTom extraction file is retrievable.

11.9. Opening an encrypted extraction

To open an encrypted extraction or application, you need to enter the password. If you do not know the password, you can load passwords from a text file (dictionary).

The following encrypted extractions or applications are supported:

- BlackBerry encrypted content
- BlackBerry Password Keeper
- Apple encrypted iTunes backup
- Android encrypted ADB backup
- Android encrypted memory
- TextSecure

To open an encrypted extraction:

1. Open the extraction in Physical Analyzer. Figure 1 shows an Android encrypted ADB backup and Figure 2 shows an Apple encrypted iTunes backup.

Figure 1 : Android user data encrypted

Figure 2 : iTunes backup encryption password

2. Enter the password in the space provided.

> The iTunes backup encryption password is required here to access encrypted backups, and is different from the iPhone device PIN code. Physical Analyzer sets the password to 1234 during the extraction process.

> If the iTunes backup encryption password is not available, contact Cellebrite Services for a possible encryption bypass solution.

> For BlackBerry encrypted content, you need to enter the password that matches the displayed SHA-1 hash.

–Or–

Click **Load from file** to load a list of passwords from a text file (dictionary). The file must include a list of passwords, with each password on a separate line.

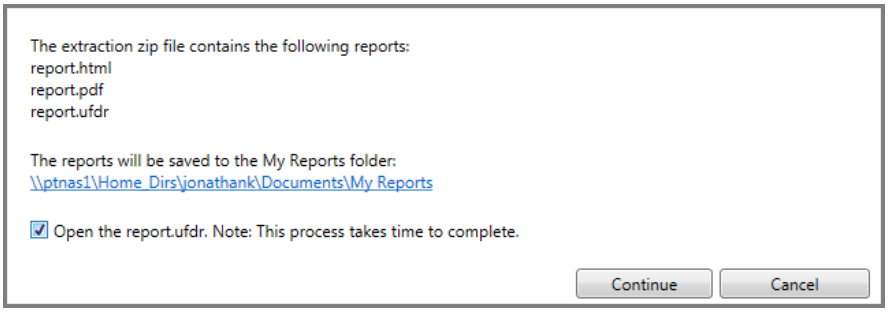
3. Click OK.

11.10. Opening an encrypted zip file

Physical Analyzer can open encrypted zip files created by Cellebrite Responder. The zip file can contain HTML, PDF and UFDR report files. Only the UFDR file can be opened. To open an encrypted zip file, you need to enter the password.

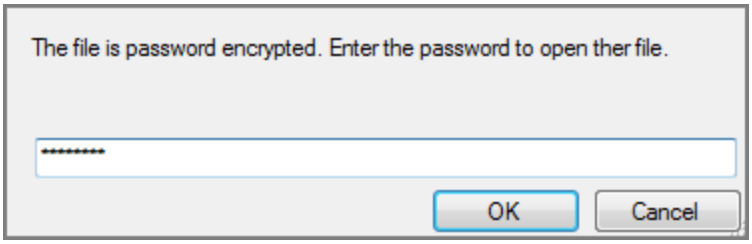
To open an encrypted zip file:

1. Open the extraction in Physical Analyzer. The following window appears.



   The window indicates where the report files will be saved.

2. To open the report.ufdr file, select the **Open the report.ufdr** check box.
3. Click **Continue** to save the report files to the location indicated. The following window appears.



> You can change the location under **Settings** > **Report Defaults** > **Default folder**.

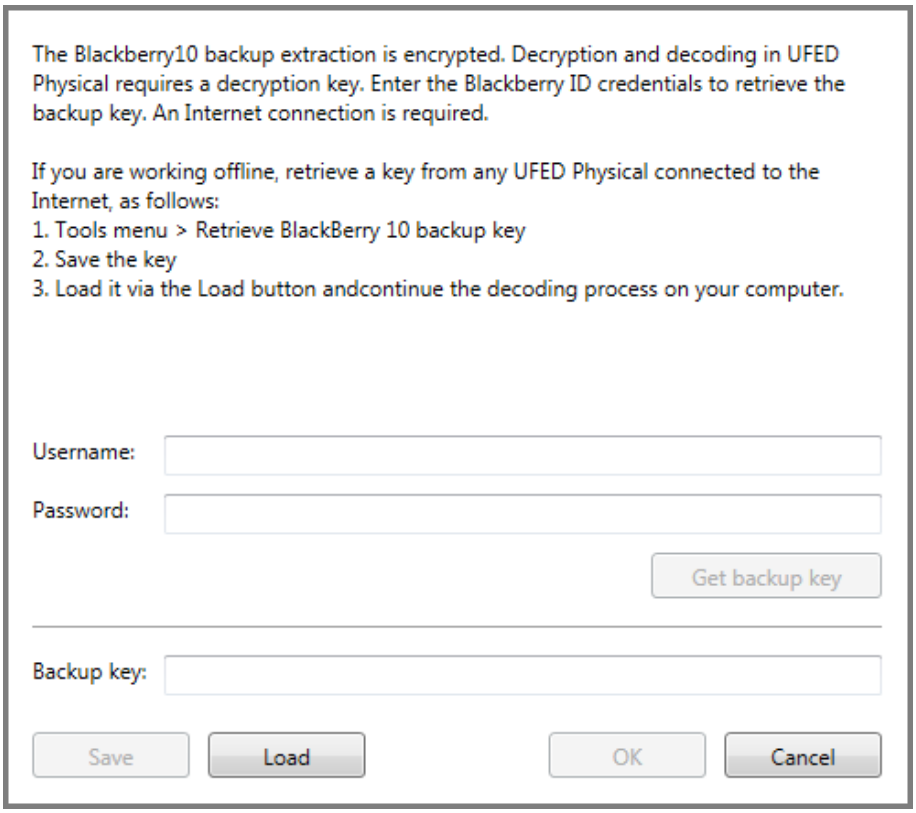
4. Click OK.

11.11. Extraction and decryption of BlackBerry backup files

You can decrypt the backup file from BlackBerry 10 devices. This feature is part of the file system extraction. Use Physical Analyzer to retrieve the BlackBerry backup key and decrypt the backup data.

To retrieve a key with an Internet connection:

1. Open a file system extraction of a BlackBerry 10 device. During the decoding process, the following window appears:



2. Enter the BlackBerry ID credentials and click **Get backup key**.
3. To save the key for future use, click the **Save** button.

To retrieve a key without an Internet connection:

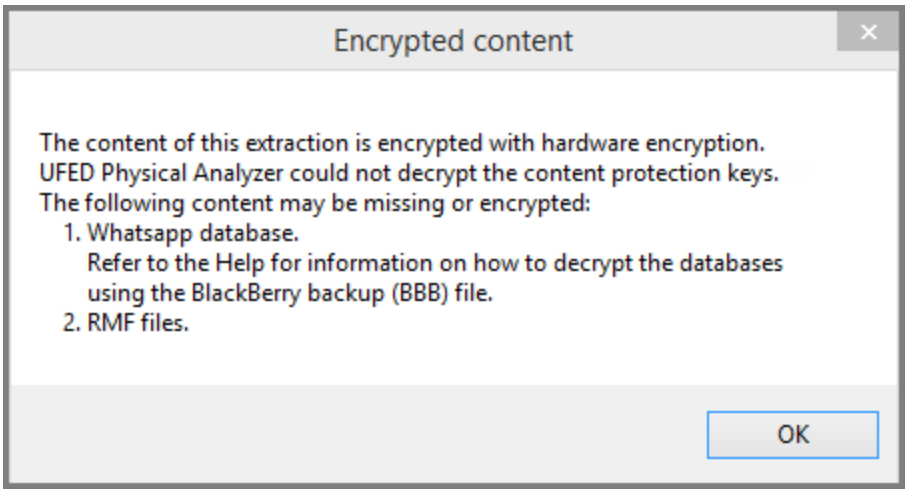
1. If an Internet connection is not available, you can retrieve a key on any instance of Physical Analyzer connected to the Internet. Go to **Tools** and select **Retrieve BlackBerry 10 backup key**.
2. Enter the BlackBerry ID credentials and click **Get backup key**.
3. Click **Save** and load the key on the Physical Analyzer not connected to the network to continue with the decoding process.

11.12. WhatsApp decryption on BlackBerry databases

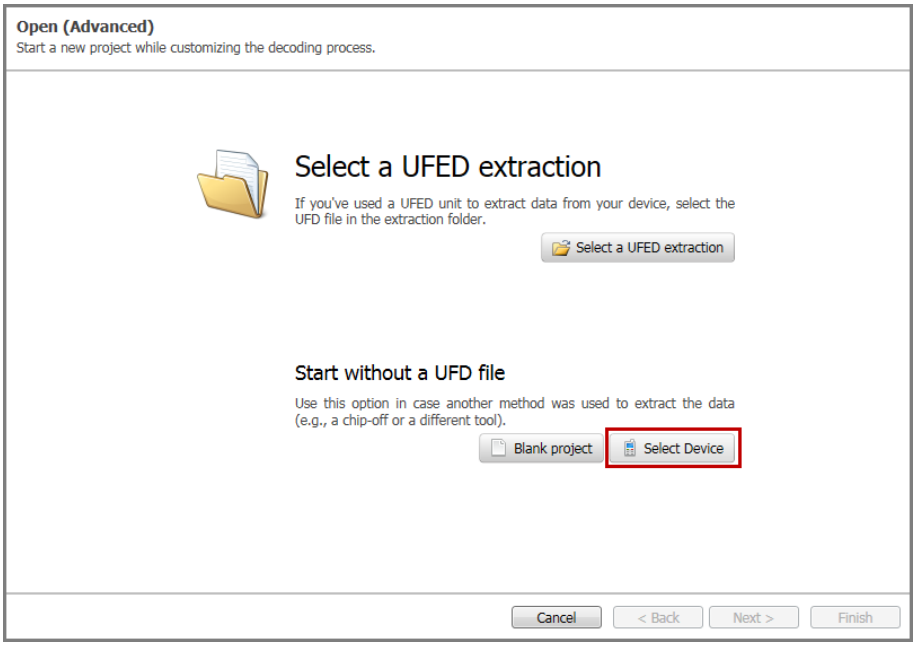
This section provides information when the WhatsApp databases on OS 7 BlackBerry devices cannot be decrypted, because one of the keys which is essential to the decryption process is missing. In this case, the key can be recovered using the following procedure.

To decrypt WhatsApp on BlackBerry databases (OS 7):

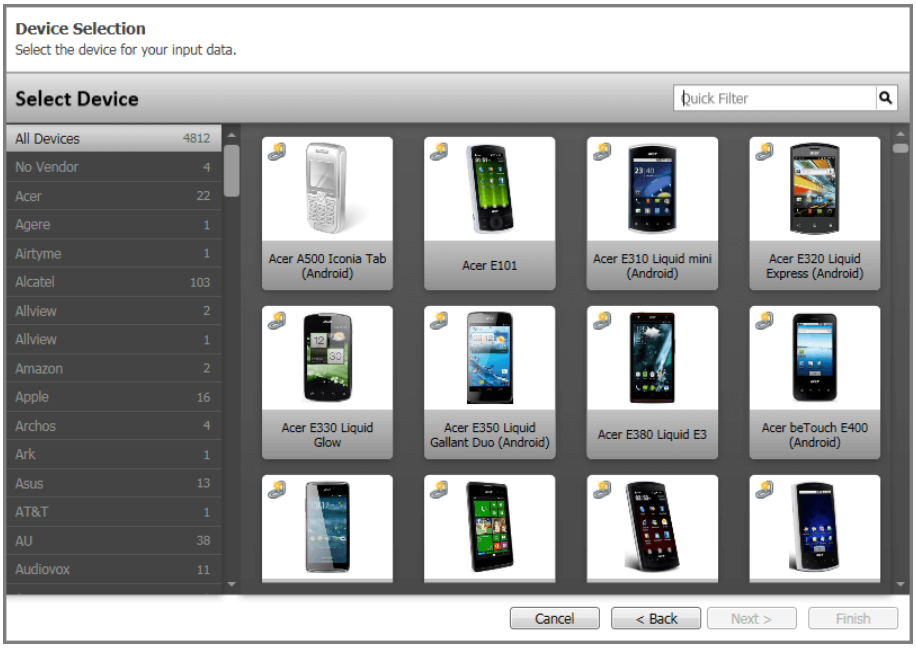
1. If you run the physical extraction, you will receive a message that the WhatsApp databases cannot be decrypted. You will be able to see messageStore.db files in the file system, but they are encrypted.



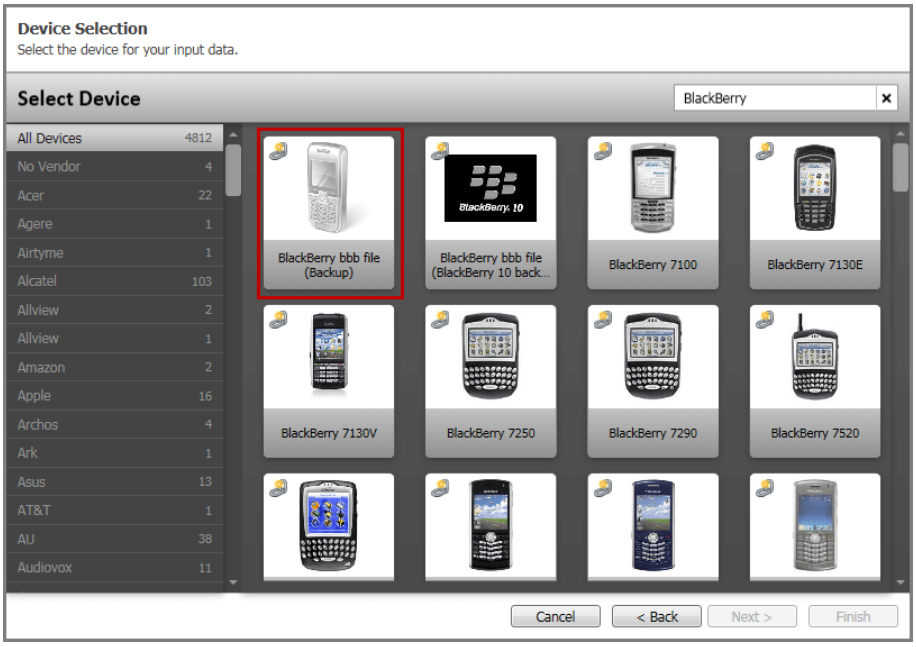
2. Create a BBB file (BlackBerry backup file) using the BlackBerry software installed on a PC.
3. Click **Open (advanced)** to load the BBB file into Physical Analyzer. The following window appears.



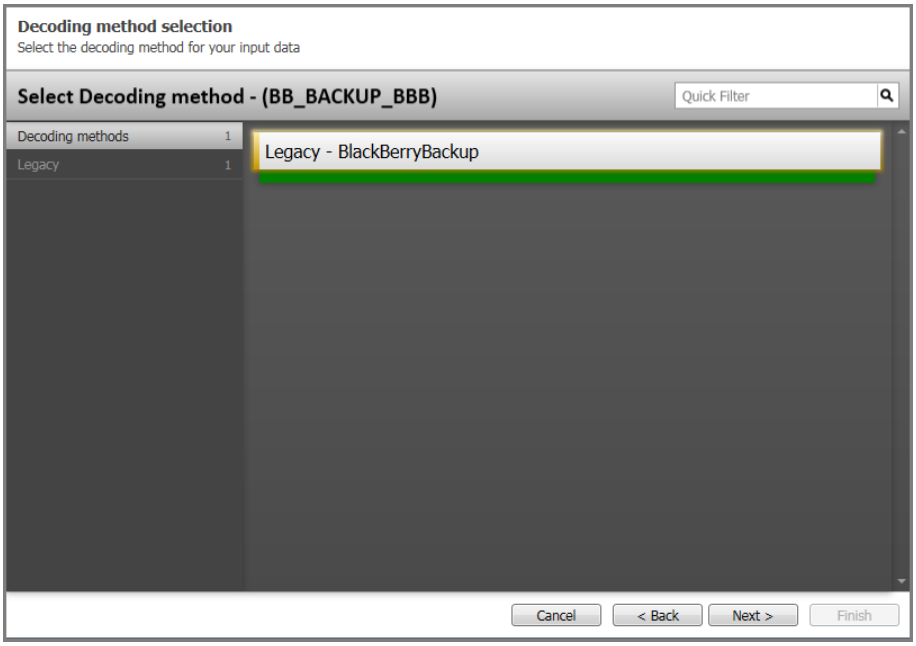
4. Click **Select Device**. The following window appears.



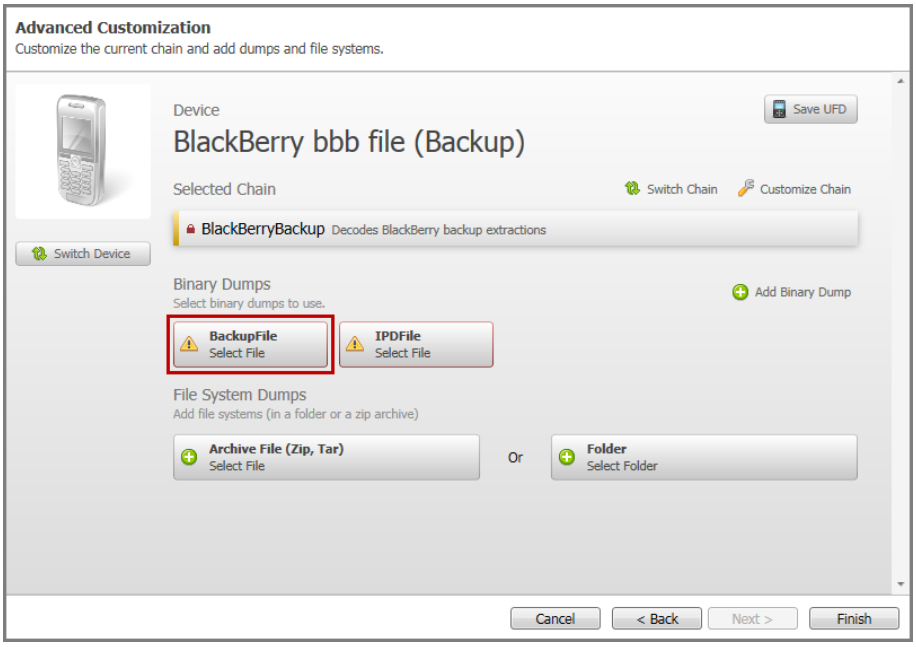
5. Select BlackBerry on the left or search for BlackBerry in the quick filter search.



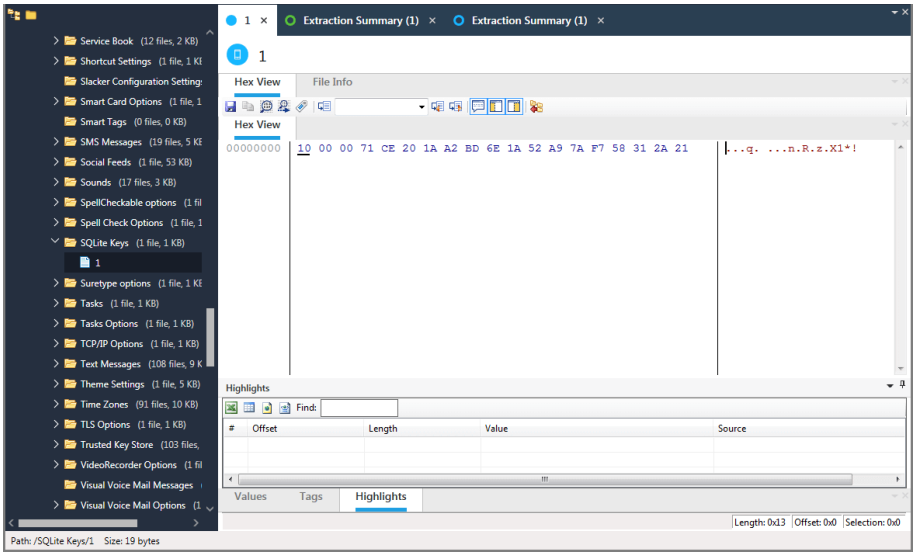
6. Select **BlackBerry bbb file (Backup)** and click **Next**. The following window appears.



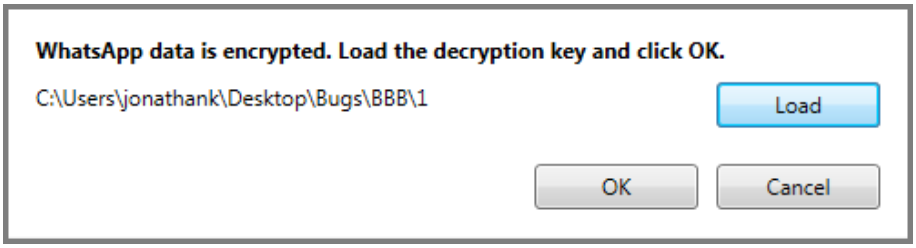
7. Click **Next**. The following window appears.



8. Click **BackupFile**. A browser window appears.
9. Click **Open** to load the *.bbb file.
10. Click **Finish**. Some of the WhatsApp files are already automatically decoded.
11. In the search box type SQLite Keys/1 and open the file in the Hex View. The following window appears.



12. Click to save the file. The file should be 19 bytes long.
13. Run the physical extraction and load the saved "1" file in the WhatsApp decryption key window. This window appears after the Encrypted content window.



14. Click OK. Chats from the decrypted WhatsApp databases should now be available.

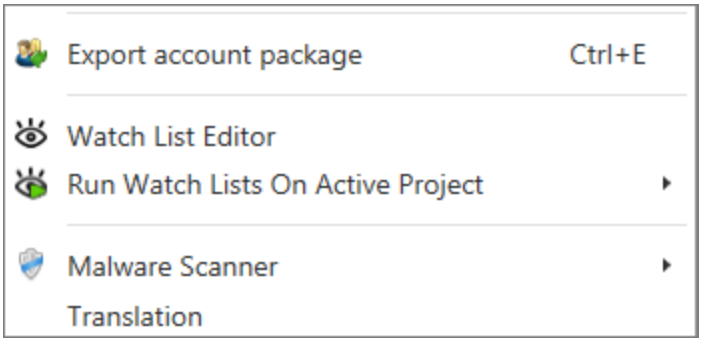
11.13. Exporting an account package from Physical Analyzer

Export an account package to extract cloud accounts using tokens.

> This step is only necessary if UFED Cloud is installed a separate machine than Physical Analyzer.

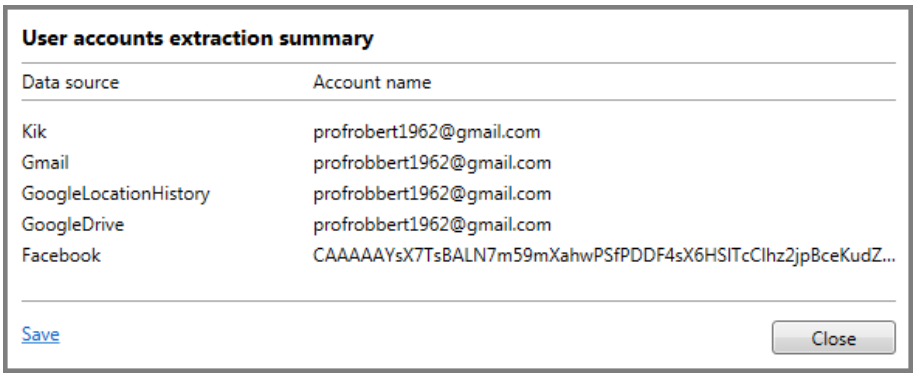
To export an account package:

1. Open an extraction in Physical Analyzer.
2. Select **Tools** > **Export account package**.



The Save As window appears.

3. Click **Save** to save the Export file (*.ucae) file. The following window appears.



4. Click **Save** to save a text file summary of the extracted user accounts, or click **Close** to complete the process. (The summary may be useful when preparing search warrants, or to share with other investigators.)

> Multiple entries for the same data source may relate to different accounts that were used on the device, or to previous login information for the same account.

11.14. Media classification

Physical Analyzer's Media classification feature allows you to classify images and videos based on categories that are relevant to the case.

When this feature is enabled, machine learning algorithms will automatically scan and classify all images and videos in your case to the following categories:

Topic	Categories
General	» Flags » Food » Jewelry » Maps
Money	» Credit cards » Money (cash)
People	» Faces » Gatherings » Hand hold object » Nudity » Tattoos
Places	» Beach » Hotel rooms » Pool » Restaurant
Substance	» Cigarettes Drugs
Tech	» Camera » Smartphones
Textual	» Barcodes and QR codes » Documents » Handwriting » Invoices » Photo IDs » Screenshots

Topic	Categories
Transportation	» Cars » License plates » Motorcycles » Vehicle dashboards
Violence	» Fire and explosion » Upskirt
Suspected CSA (Child Sexual Abuse)	

Media Classification is CPU-based and requires additional processing time, so a newer CPU (generation 6 and higher) is required. If your CPU is not compatible with our Media classification engine, you can still use it, but processing time will take much longer.

11.14.1. Running Media classification

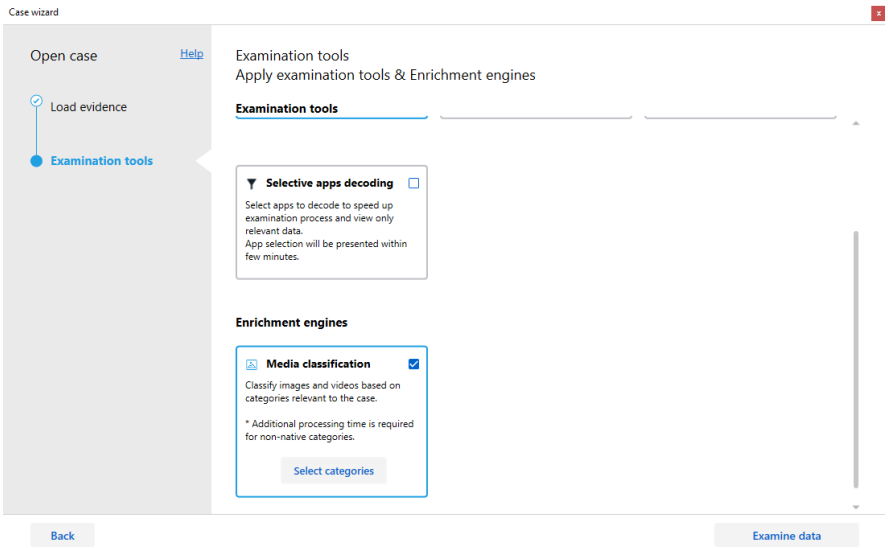
You can select to run Media classification in the Examination tools step of the Case wizard. See Examination tools (on page 69).

Specify which type of media classification and which specific categories to run on the case.

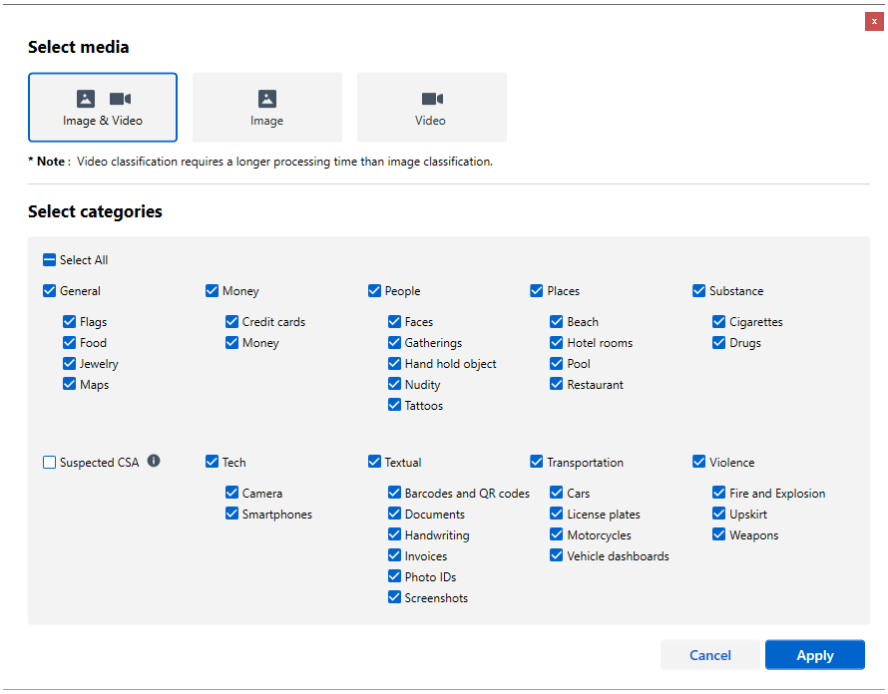
Running Media classification requires additional processing time.

To run Media classification after project has already loaded see Running Media classification on demand (on page 352).

1. In the Case wizard, under Enrichment engines, select **Media classification**.



2. Click **Select categories**. The following window appears:



3. Select the type of media classification to run:
   - Image and video
   - Images only
   - Videos only

> Video classification requires a longer processing time than image classification.

4. Select or unselect the categories relevant to the case.

> By default, all categories are selected except for Suspected CSA.

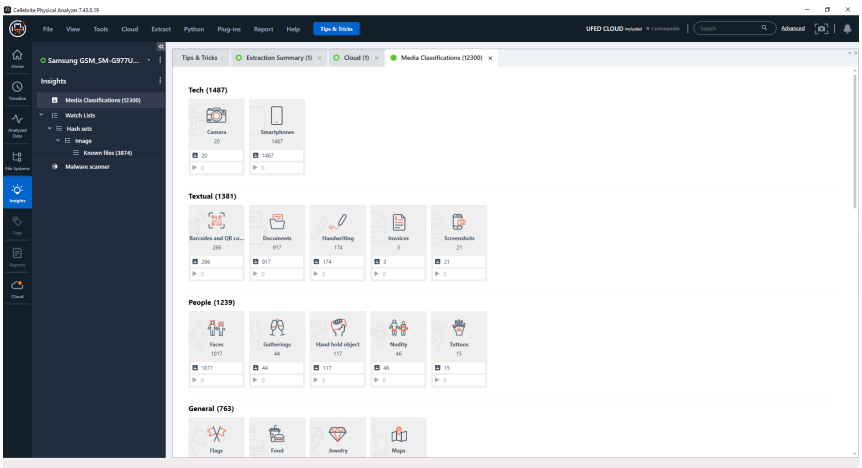
> Running the Suspected CSA category may increase process time and memory consumption. Use a GPU card (NVIDIA® GPU card with CUDA© compute capability 3.5 or higher) to boost the speed of this process.

5. Click **Apply**.

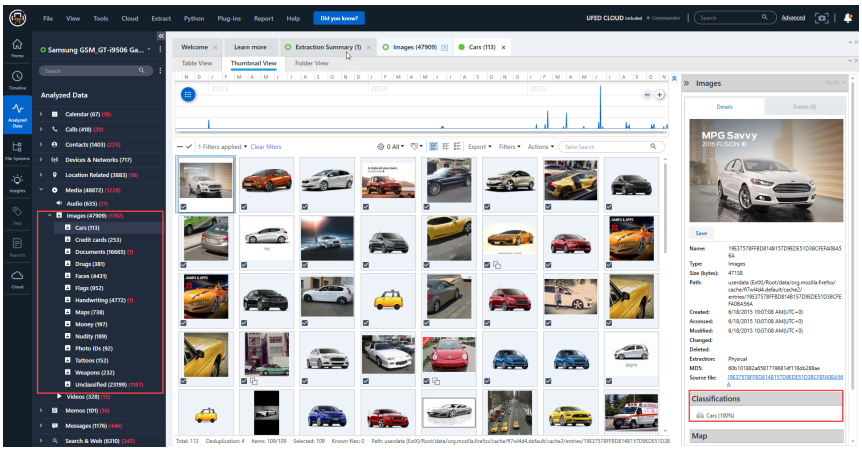
11.14.2. Viewing and analyzing classified media

Once the project is loaded into Physical Analyzer, there are three ways to view images according to their classification.

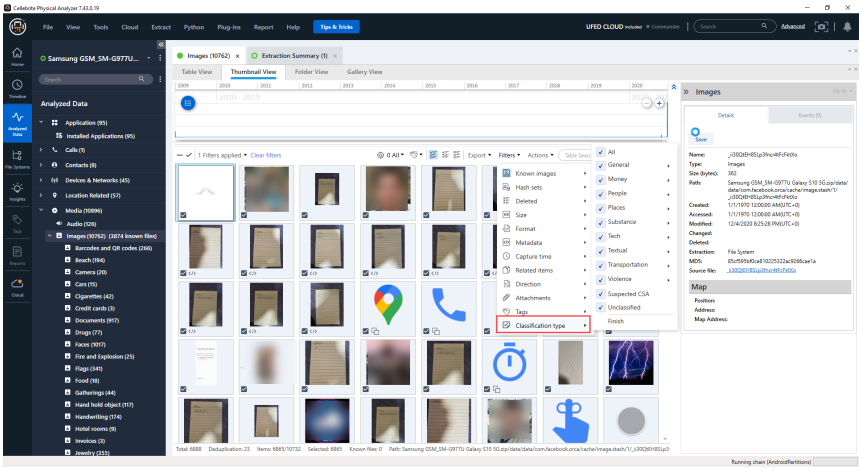
1. **Insights**
   a. Go to the Insights menu item.
   b. Double click **Media classifications**.
   c. For each category click to view the images and/or videos.



2. Analyzed data tree
   a. Click on the Analyzed data menu item.
   b. Under **Media** tree item, double click **Images** or **Videos**.
   c. Double click a category to view the media.



3. Filtering the media by classification type
   a. Click on the Analyzed data menu item.
   b. Under **Media** tree item, double click **Images** or **Videos**.
   c. Click **Filters > Classification type.**.
   d. Select or unselect the categories to display.

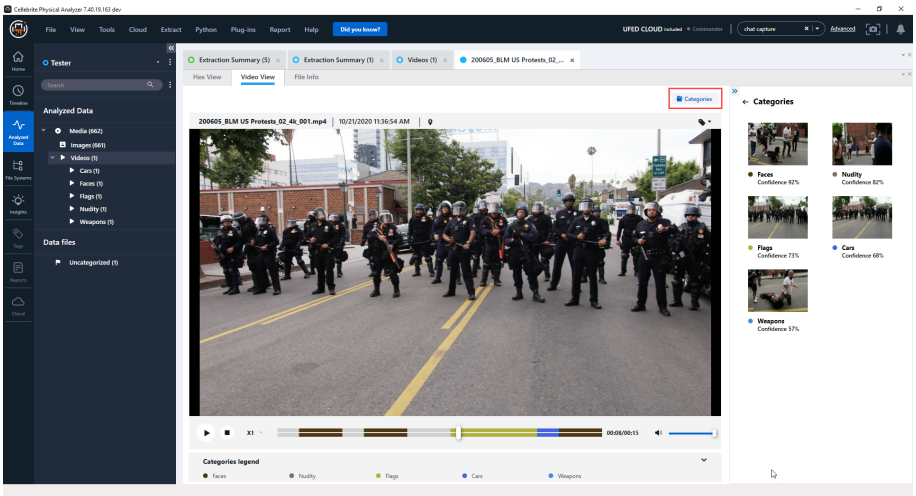


Viewing classified videos

Video classification allows users to locate valuable information without the need to view entire videos. When a category has been found in the video, you can jump directly to the frame in which it can be seen.

To locate frames containing classified categories

1. Double click the video to open in new tab.
2. Click **Categories**. The classified categories and their confidence score (See Media classification score control (below)) are displayed in the right panel.
3. Click on a category to locate the related frames.



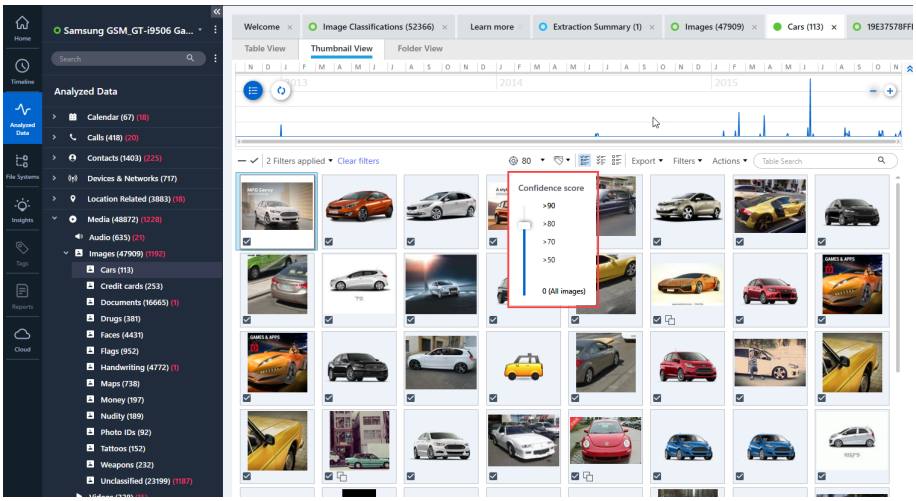
The video progress bar is color coded to show where categorized frames appear. See the Categories legend at the bottom of the screen for reference.

Media classification score control

Each classified image and video is given a score (0-100%) based on classification accuracy. When viewing specific categories, the items are sorted from highest to lowest score.

You can use the classification score filter to display results within a certain range.

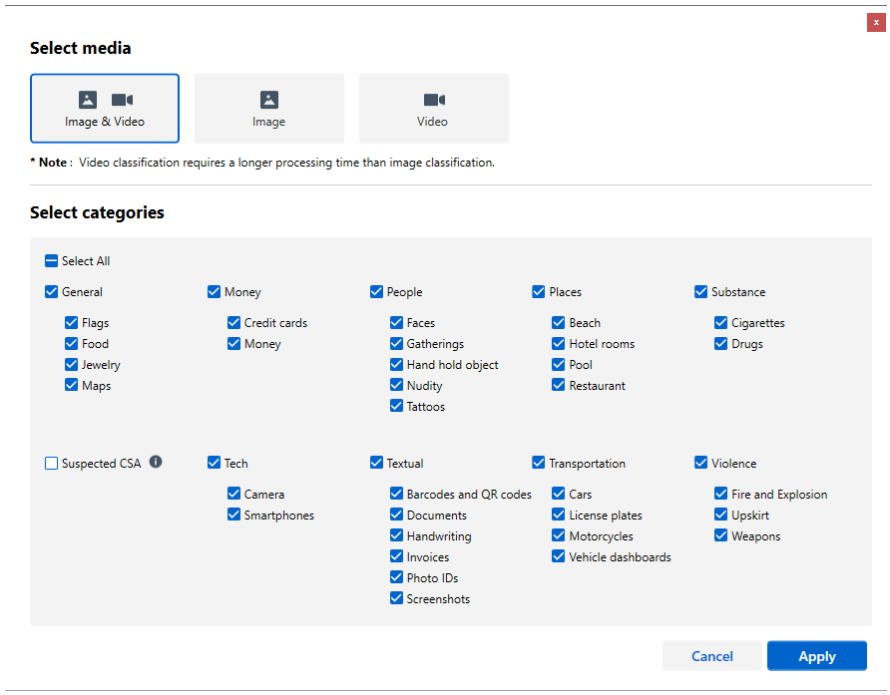
In the example below, the classification score filter is set to display only those results with a score of 80% or higher. This filters out less accurate results.



11.14.3. Running Media classification on demand

In the case that Media classification was excluded or only partially run (for example, only Image classification was selected) when loading the case, you can run it after the project has loaded.

1. Go to **Tools > Review engines > Media classification.** The following window appears:



2. Select the type of media classification to run:
   - Image and video
   - Images only
   - Videos only
3. Select or unselect the categories relevant to the case.
4. Click Apply.

11.15. Selective apps decoding

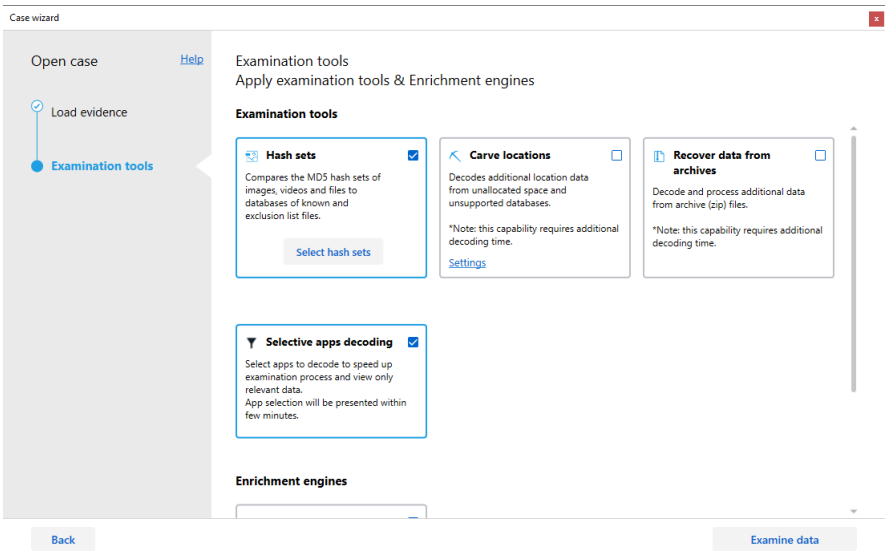
This capability enables you to select apps that are installed on your examined device to decode and review. By selecting only the relevant apps, processing time is shortened and you can review the evidence faster by reducing unnecessary data.

The list of the device's installed applications is generated through a Cellebrite UFED extraction or through running a short pre-stage within Physical Analyzer and choose the selectively parsed applications.

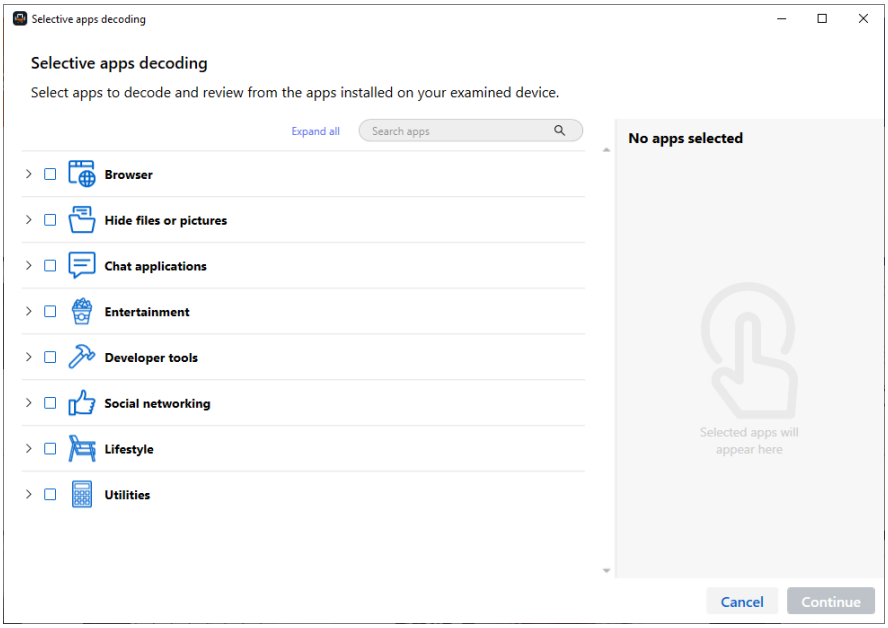
11.15.1. Selecting apps to decode

You can select to run Selective apps decoding in the Examination tools step of the Case wizard. See Examination tools (on page 69).

1. In the Case wizard, select **Selective apps decoding**.

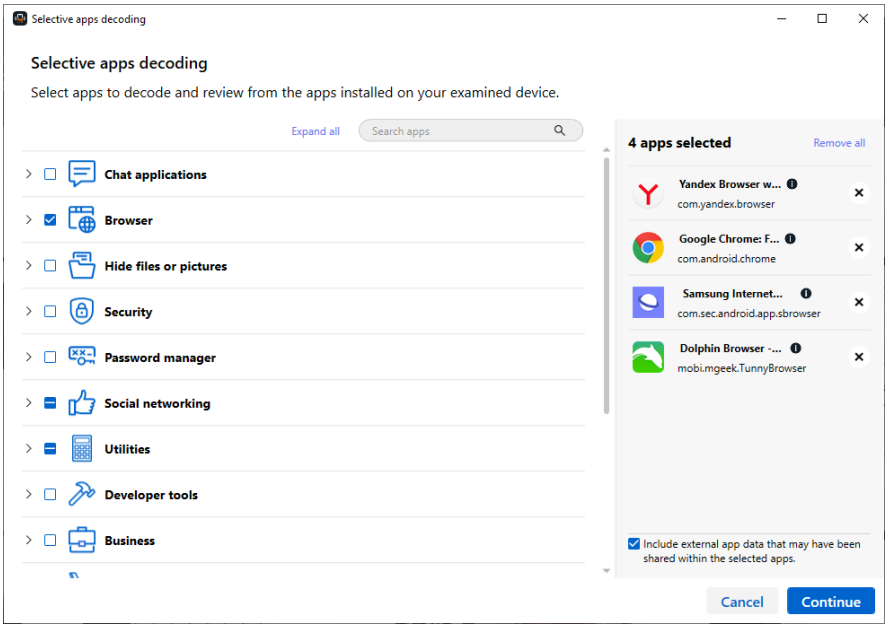


2. After clicking **Examine data** and the decoding begins, the following window appears:



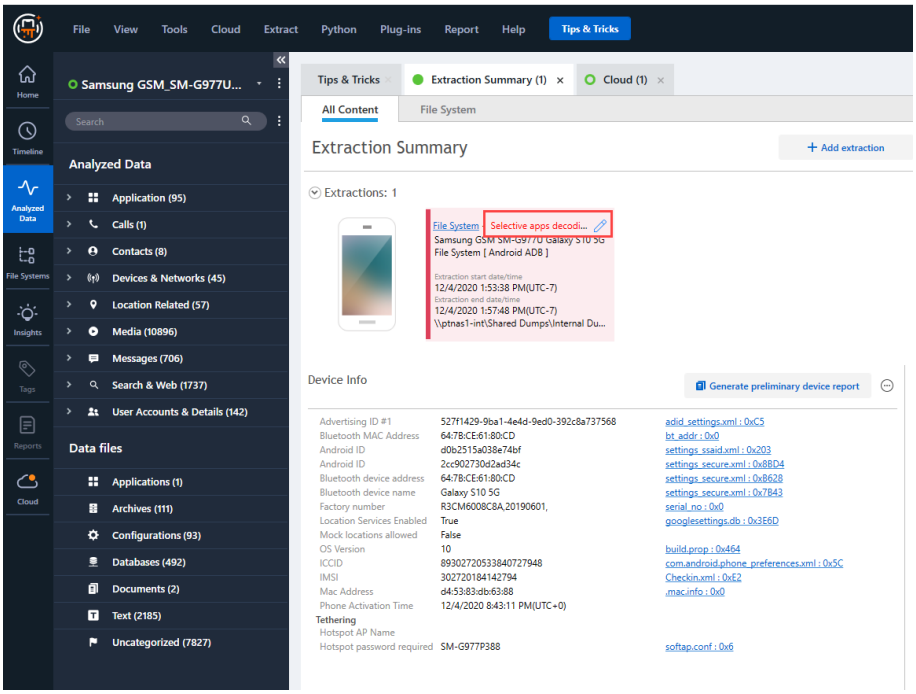
> It may take a few minutes for the Selective apps decoding window to appear.

3. Select an app category to include all apps, or click on the arrow to select specific apps within a category.
4. Once selected, the apps appear in the right pane.



5. If you wish to include external app data that may have been shared within the selected apps, select the check box.
6. Click **Continue** to begin decoding.

Once the decoding is completed, there is an indication in the Extraction summary that Selective decoding was used:



Important Notice: For the decoding process to complete successfully, native phone data may be decoded and displayed in addition to the applications selected during the Selective decoding flow.

11.16. Carving images

Perform image carving to retrieve jpeg image files or fragments that are incomplete or corrupt, signifying that they have been deleted by the user. Image carving retrieves the images and rebuilds them as much as possible.

Perform image carving on demand; carving is not performed when Physical Analyzer opens the physical extraction.

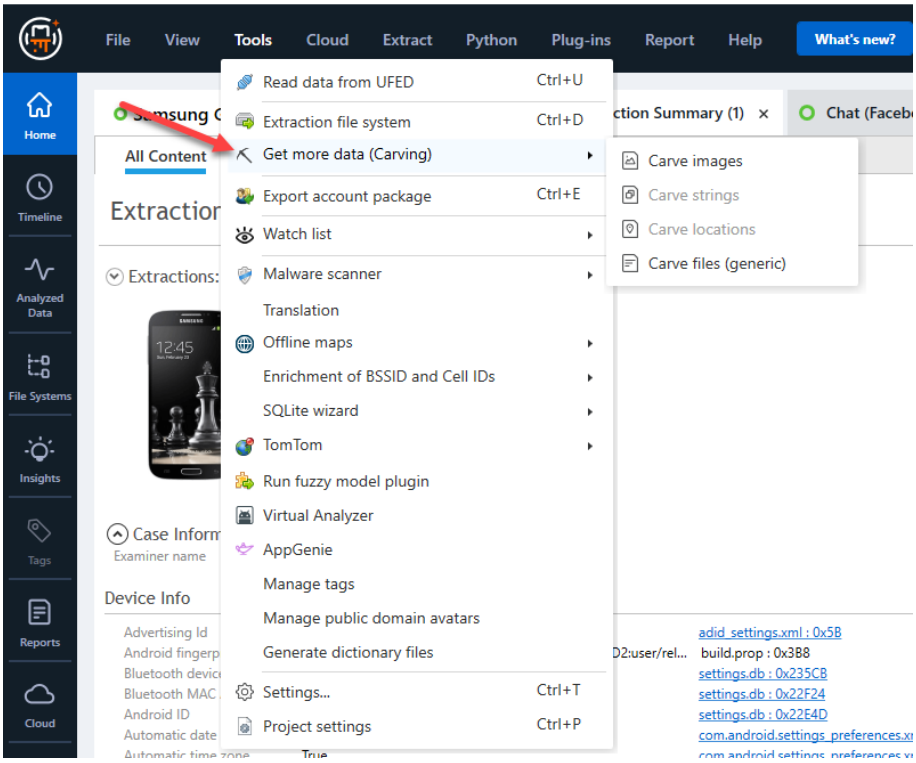
> Image carving is only available for physical extractions.

Image carving can take some time to process. While processing, you can work in parallel in Physical Analyzer.

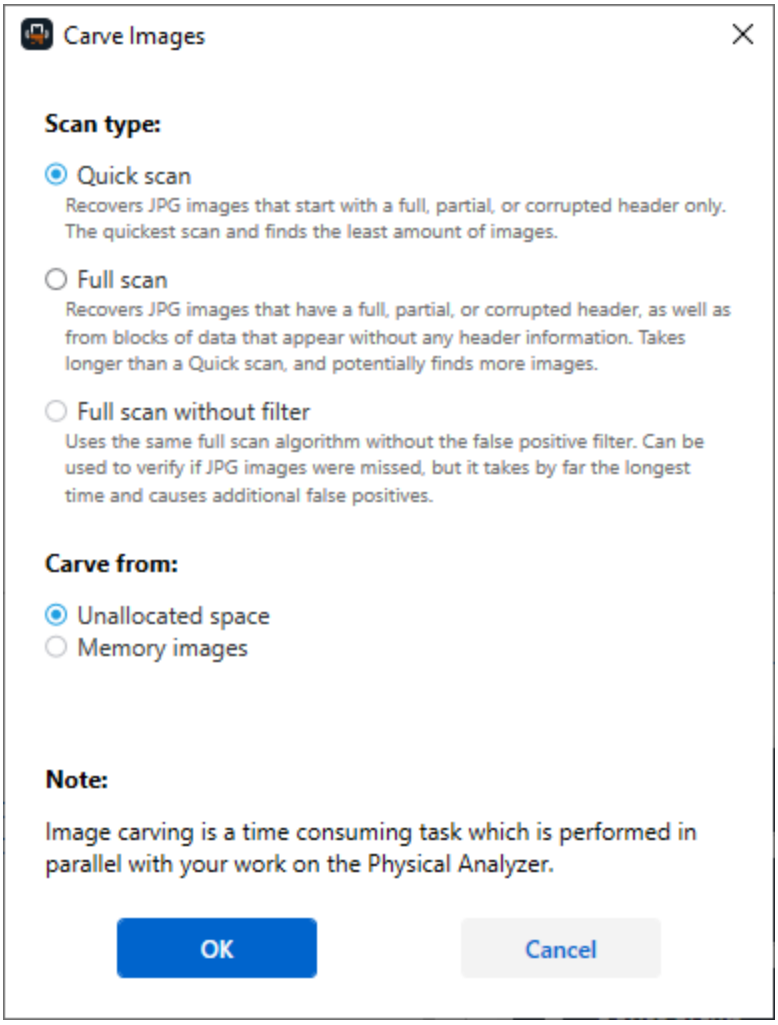
11.16.1. Scanning for carved images

To scan for carved images:

Go to **Tools > Get more data (carving) > Carve images.**



The following window appears:



Select the scan type:

Quick scan- This scan has three stages, where Physical Analyzer tries to recover images that start with a full, partial, or corrupted header only.

Full scan - This scan has five stages, where in addition to recovering images that have a full, partial, or corrupted header, Physical Analyzer tries to recover images from blocks of jpeg data that appear without any header information. A full scan takes longer than a quick scan, and potentially finds more images.

Full scan without filter - This scan uses the same Full scan algorithm without the false positive filter. It can be used to verify if images were missed, but it takes by far the longest time and causes additional false positives.

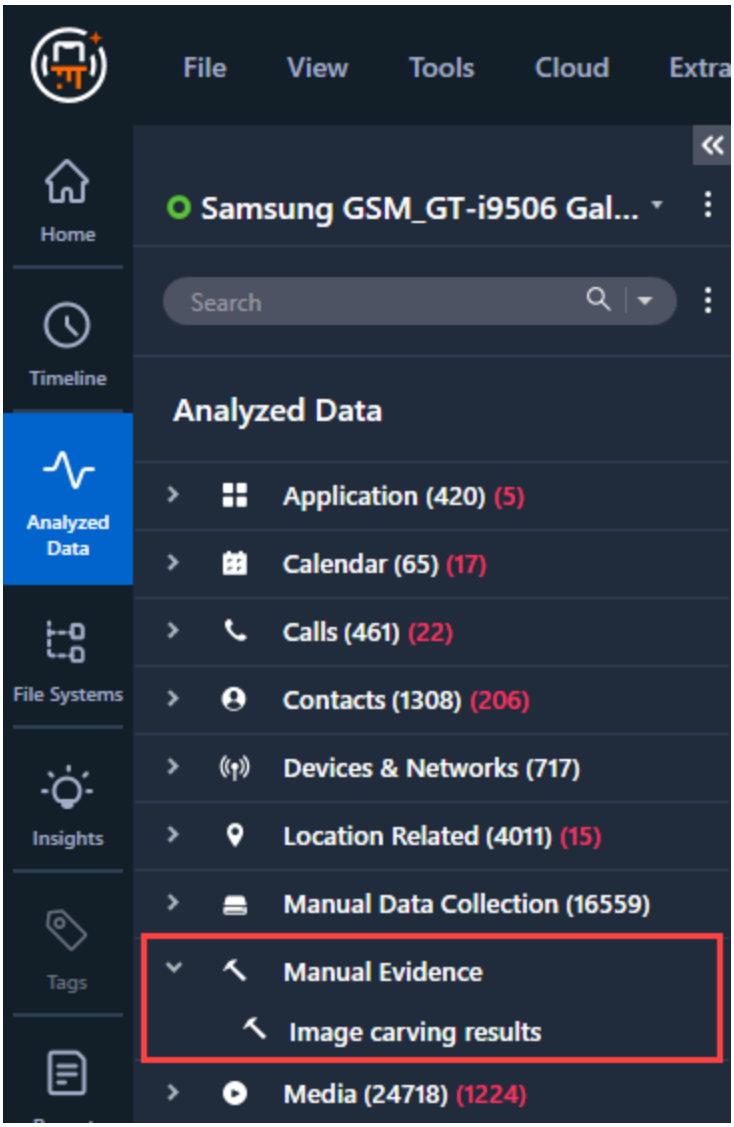
Select from where you want to carve the images:

Unallocated space - scan unallocated memory space.

Memory images - select all images that you want to scan.

Click Ok.

The scan begins. Results are shown in **Manual evidence**> **Image carving results**tree item.



11.16.2. Working with carved images

Open data display tabs for all the carved images, for individual carved images, and extract the images to your computer.

To view all the found images in the project tree:

» Click to expand the **Carving** > **Images** tree item.

To open a data display tab for an individual image:

» Double-click the image in the project tree.

For more information on working with images, see Viewing image files (on page 124).

To extract (dump) the carved images to your computer:

1. Right-click the **Carving** > **Images** tree item and select **Dump**.

2. In the Select Folder window, browse to the desired folder, and click **Select Folder**.

11.17. Carving locations

The Carve locations feature allows you to decode additional location data from unallocated space and unsupported databases. The carver allows you to either search for additional locations, up to three of the most visited areas, or any other custom area.

> The carving results may produce many false positive events.

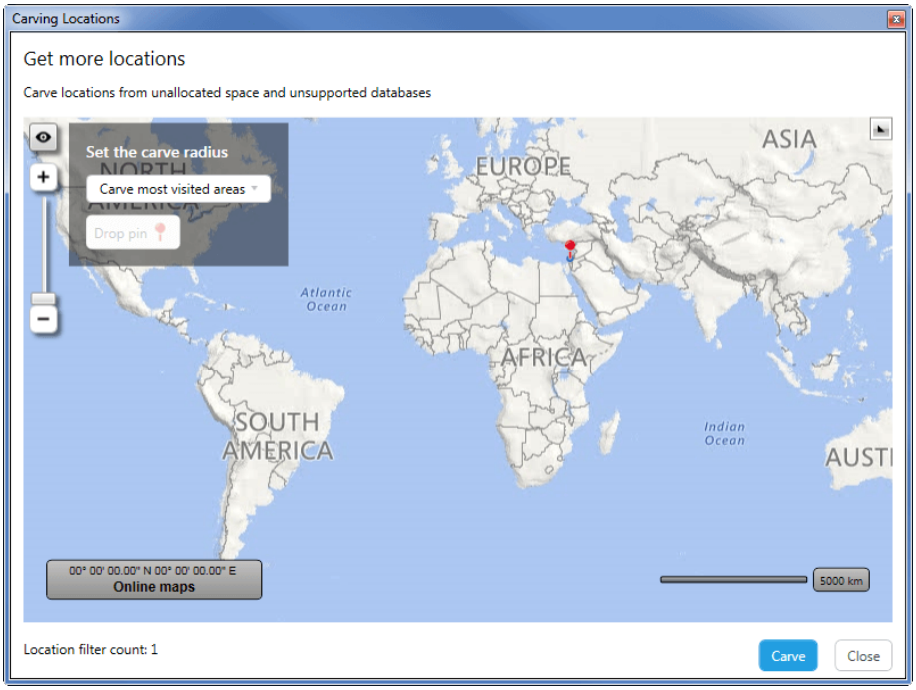
To carve for locations:

1. Select **Tools** > **Get more data (Carving)** > **Carve locations**.

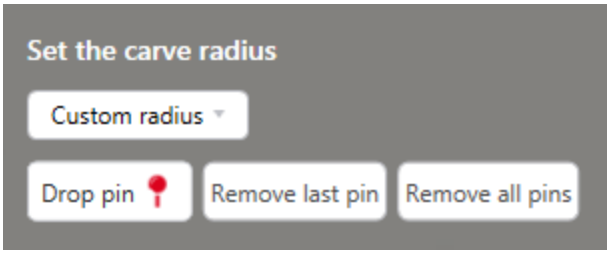
   –Or–

   Open the Device locations and click Carve locations (⛏).

   The following window appears.



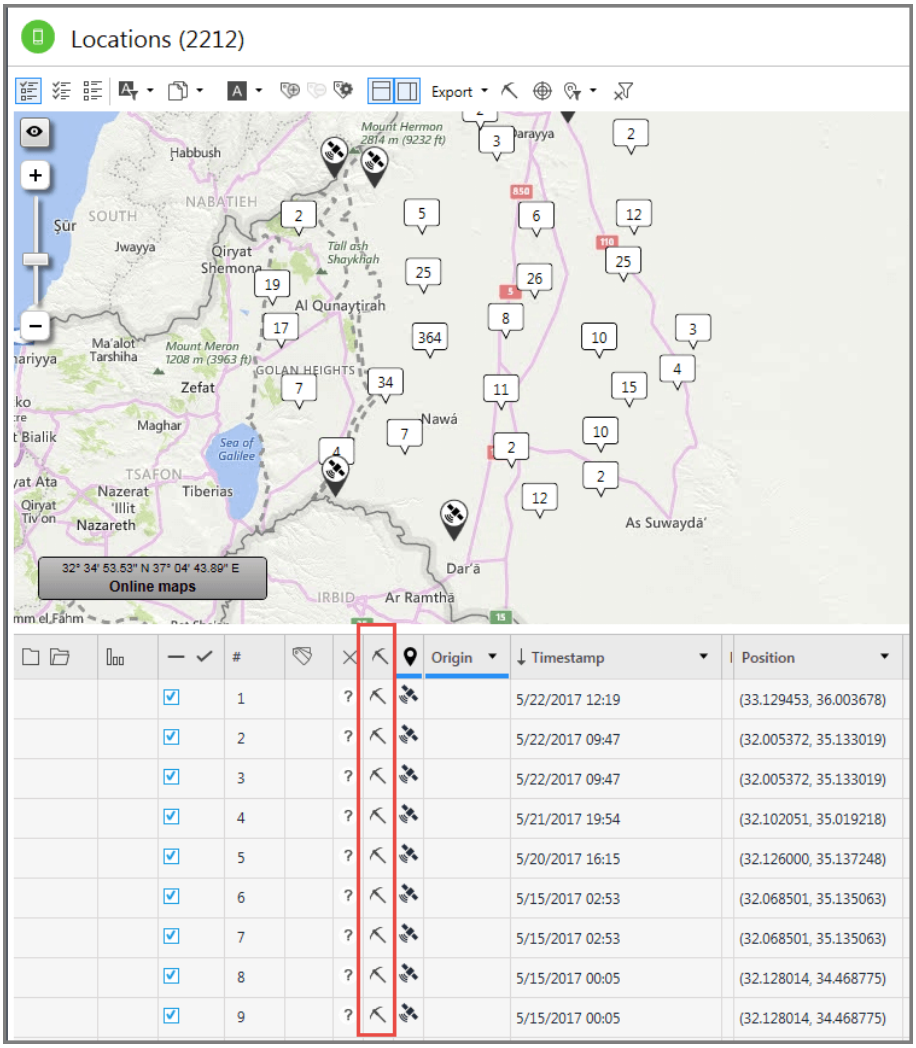
2. From the carve radius are, select:
   - **Carve most visited areas:** Search for additional locations based on up to three most visited areas.
   - **Custom radius:** Use the **Drop pin** to set an initial point, then move to mouse set the radius, click when done. After setting then pin you can drop additional pins, remove the last pin or remove all pins.



3. Click **Carve**. A progress bar below the graph indicates the carving progress. A message is displayed when the process completes and the total number of locations that were found.

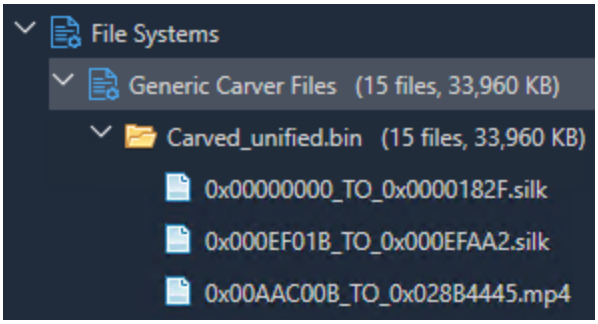
> Closing the Carving Locations window once the carving process is running will not affect the carving process.

Results are displayed under the Device locations tree item in the Carving column. An example is displayed next.



11.18. Generic file carver

Decode additional file data from unallocated space. Supported formats: MPEG, Amr, Silk, Mus, Plist, RTF, PDF, and Doc. Carving results are displayed under **File Systems** > **Generic Carver Files** and under **Data Files** marked with a carved icon .



> MPEG formats: Mp4, 3g2, 3gp, F4a, F4b, F4p, F4v, Jp2, Jp20, M4a, M4b, M4p, M4v, Ross, Dvb, Jpm, Jpx, Mj2, Mj4, Mqv, Mov.

To active generic file carving:

» Select **Tools** > **Get more data (Carving)** > **Carve files (generic)**.

11.19. Verifying hash values

A hash value is a unique and compact representation of a piece of data, which can be used for integrity protection due to the fact that it is computationally improbable to find two distinct inputs that hash to the same value.

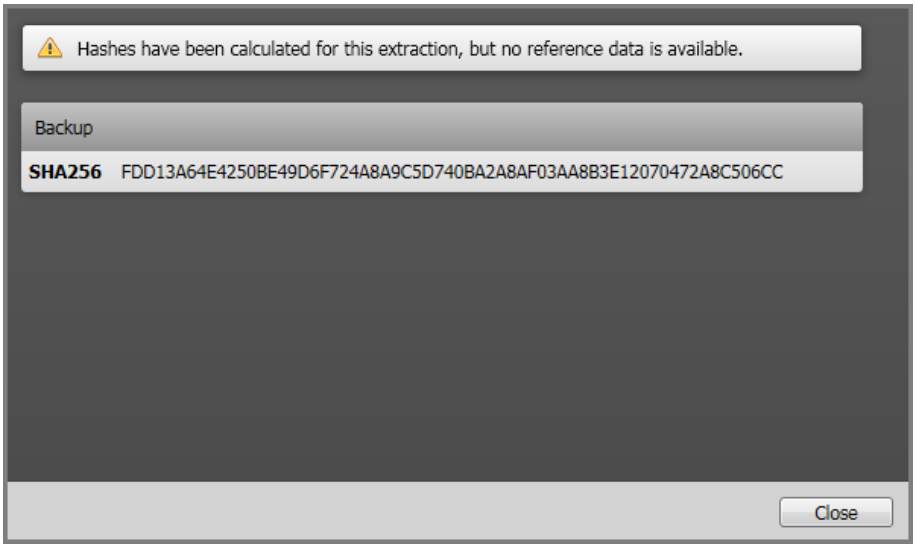
Comparing a reference hash value that was generated during the extraction process for each binary extraction against their calculated hash values enables you to verify the integrity of the binary extractions you received.

To verify the hash values:

1. In the project **Extraction Summary** tab, do one of the following:
   - If hash information is available for the project, click **Verify**.
   - If hash information is not available for the project, click **Calculate hashes**.

   The hash information is calculated or verified. If no reference data is available, a **Hashes have been calculated for this project, but no reference data is available** message is displayed in the **Image Hash Information** section of the **Extracted** Summary tab.

2. Click **View Details**.



   The Image Hash Details dialog displays the comparison result of the reference and calculated hash values of each image.

   - Verified indicates matching values.
   - Bad Verification indicates the images do not match.

11.20. Accessing WhatsApp Web data

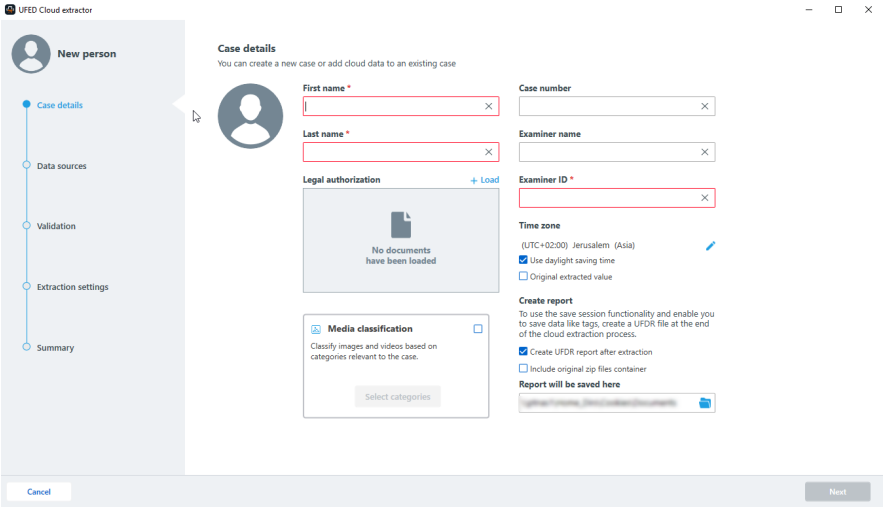
Extract WhatsApp Web data such as contacts, user account, chats data, and chat instant messages including attachments, shared contacts, locations, etc. by scanning the WhatsApp QR code.

This capability requires full access to the mobile device in order to scan the QR code through the device's WhatsApp mobile app.

WhatsApp Web extraction can be performed in both Physical Analyzer and UFED Cloud.

Procedure

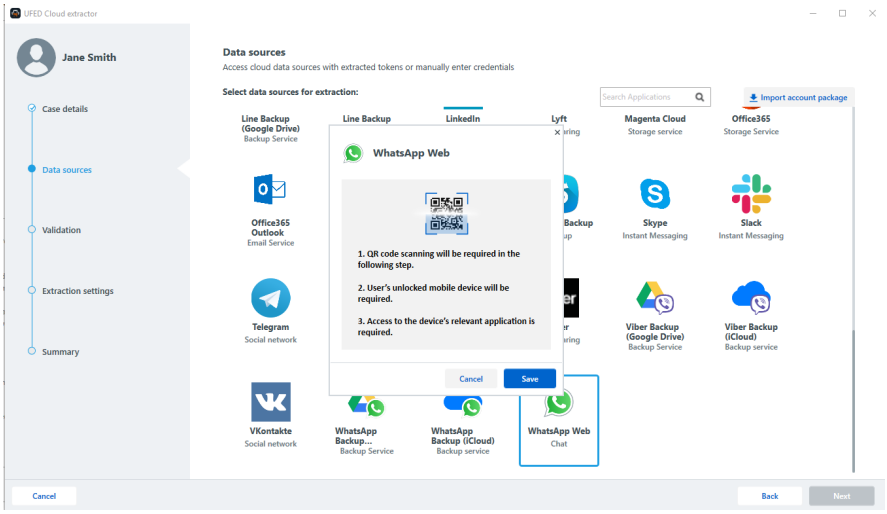
1. In the main menu, go to **Cloud > Extraction > Private cloud data.**
2. Enter the required fields.
3. Click **Next**.



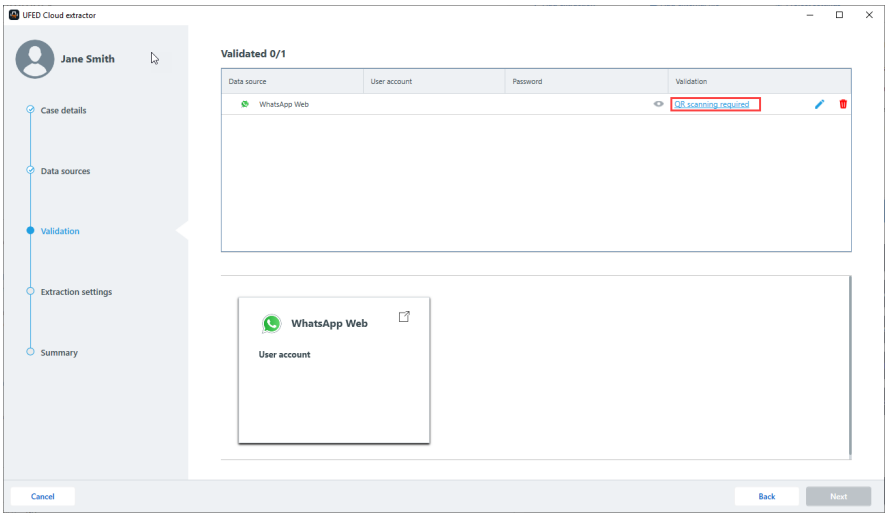
4. Select the WhatsApp Web data source.

> If you do not have a UFED Cloud license, all other data sources will be unavailable.

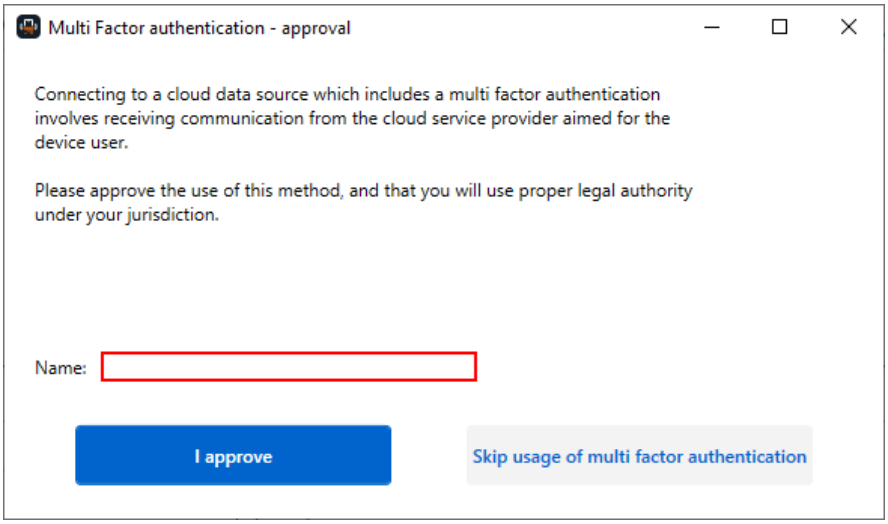
5. In the WhatsApp Web window, click **Save**.



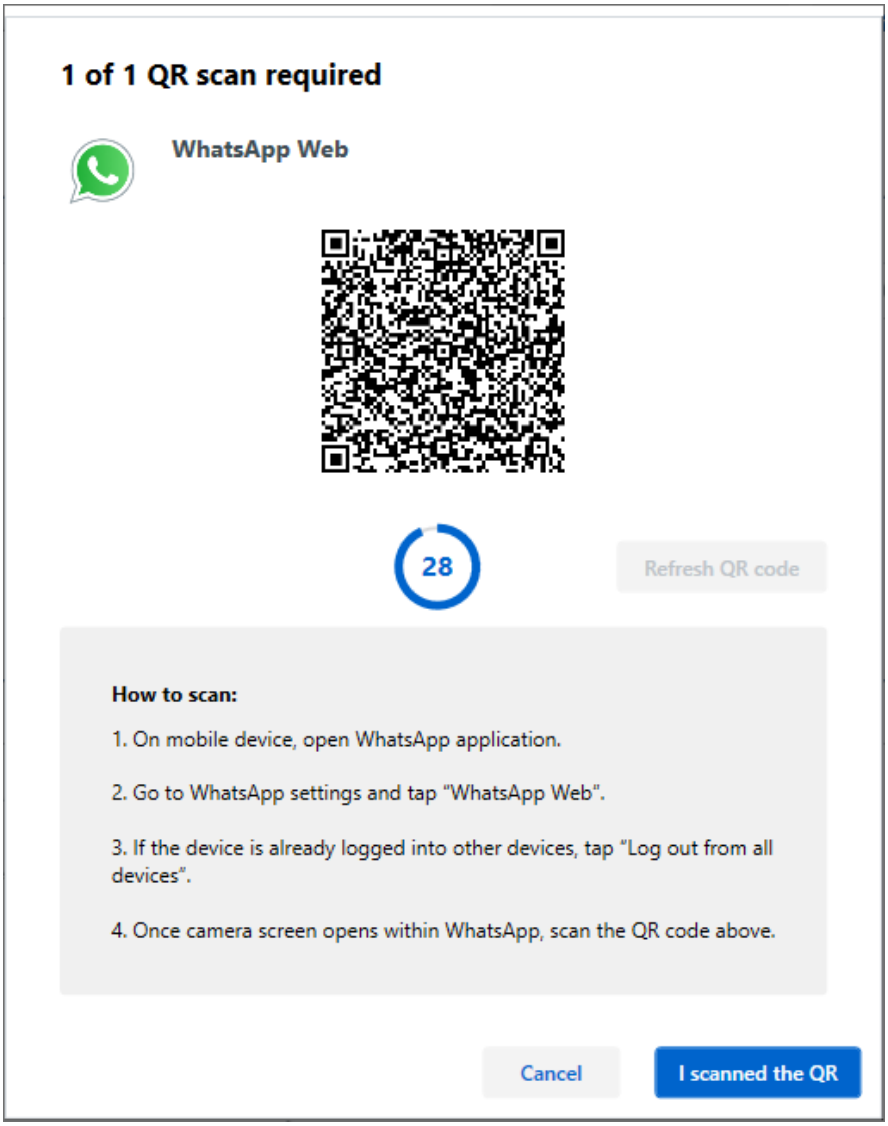
6. Click **Next**.
7. In the Validation step, click **QR scanning required.**



8. Enter your name.
9. Click **I Approve** to approve the multi-factor authentication.



10. On the device, open the WhatsApp application.
11. Go to Settings and tap **WhatsApp Web**.
12. If the device is logged in to other devices, tap **Log out from all devices.**
13. When the camera opens within the application, scan the QR code.
14. When done, click **I scanned the QR.**



15. Once validated, click Next.
16. Select a date range and click **Apply**.
17. Click **Next**.
18. In the Summary screen, click **Start extraction** to begin decoding.

11.21. Network dongle – admin procedures

The network dongle enables organizations to provide licenses for multiple UFED products, from a single, central location, to users connected to your network. This solution provides centralized license management where licenses can be easily transferred between users, and the network dongle can be updated when required.

The number of licenses and types available in the network dongle varies based on the licenses purchased from Cellebrite. The network dongle solution enables users and an administrator to manage and maintain licenses of the UFED applications, by means of an Admin Control Center.

11.21.1. Network dongle – system requirements

The minimum system requirements for the computer connected to the network dongle are as follows:

Hardware:	At least 1 GB RAM At least 1 GHz Pentium 4-compatible processor
Software:	(x86 and x64) Windows 2003 Server, Windows XP, Windows 2008, Windows 7, Windows 8, Windows Server 2012

11.21.2. Managing network dongle licenses

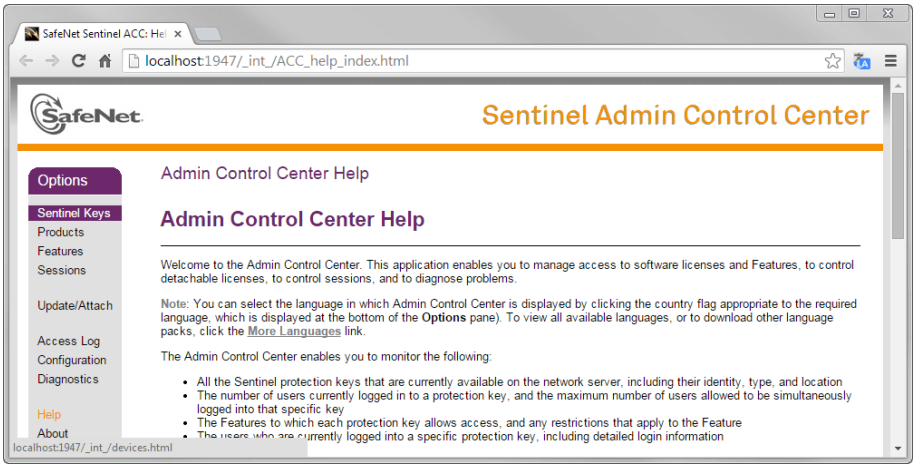
The Admin Control Center provides a single console view of all the licenses within an organization, enabling an administrator to effectively manage and maintain licenses of UFED applications. Using the Admin Control Center, administrators can update the network dongle, and view which licenses are in use and by whom, in real time, making it easy to determine and resolve license availability and compliance issues.

To manage the network dongle licenses:

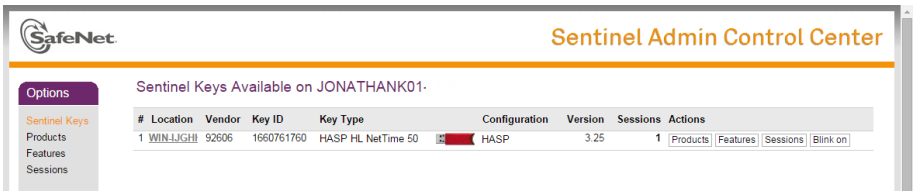
1. Use a Remote Desktop Connection to connect to the computer where the network dongle is located.
2. In a browser, enter the following: http://localhost:1947

> 1947 is the port number, which must be opened for both TCP and UDP communication.

The Sentinel Admin Control Center window appears.



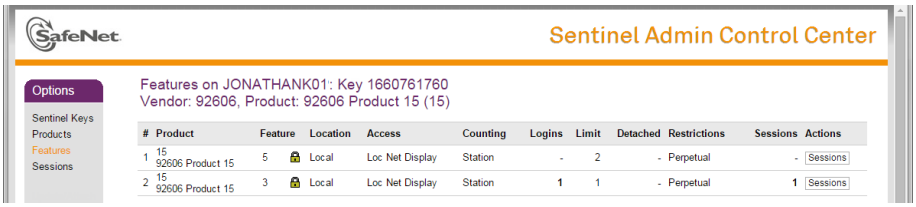
3. Click **Sentinel Keys**. The following page appears.



This page enables the administrator to identify which Sentinel Keys are currently connected to the network, including locally connected Sentinel Keys. For more information, click **Help** to display the Help for this page.

11.21.3. Features page

The Features page enables the administrator to view a list of the features or products that are licensed in each of the Sentinel Keys that are currently connected to the network, including locally connected Sentinel Keys. In addition the administrator can see the conditions of the license, and the current activity related to each feature.



The list of Feature IDs is as follows:

Feature ID	Product name
2	Cellebrite UFED 4PC
3	Physical/Logical Analyzer
4	UFED Phone Detective
5	UFED Link Analysis/Pathfinder Desktop
10	UFED Cloud

11.21.4. Sessions page

The Sessions page lists all sessions of clients on the local machine and of clients remotely logged in to the local machine. The Sessions page enables the administrator to view session data and to disconnect sessions.

To disconnect a session:

» Click **Disconnect**. The application will close and work or progress may be lost.

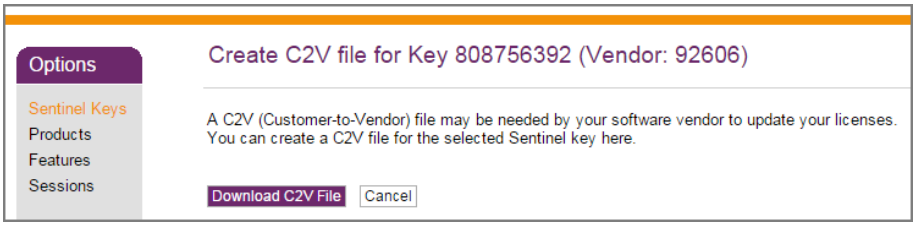
> The list of connected computers and ability to disconnect a computer may be required if a user is not available and forgets to close an application.

11.21.5. Updating the network dongle license

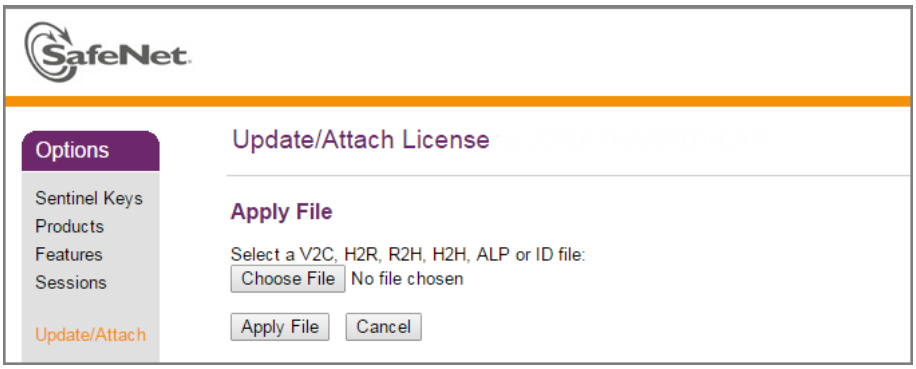
A C2V (Customer-to-Vendor) file is used to update your network dongle license. An update is required if you need to specify additional licenses, new products, features, or renewals. The C2V file needs to be sent as an attachment to Cellebrite. A V2C (Vendor-to-Customer) file, which contains the license update from Cellebrite will be returned to you.

To update the network dongle:

1. In the Sentinel Keys page click **C2V** for the network dongle that you need to update. The Create C2V page appears.



2. Click **Download C2V File**.
3. Send the file as an attachment to support@cellebrite.com.
4. After you receive the V2C file from Cellebrite, under options click **Update/Attach**. The following page appears.



5. Click **Choose file** to navigate to the file that you want to apply. The File Upload dialog box appears.
6. Select the appropriate .V2C file and click **Apply File**.

11.21.6. Standalone installation of the required drivers

The required SafeNet network drivers are installed automatically when you install supported UFED products such as Physical Analyzer, Logical Analayzer, UFED Cloud , UFED Phone Detective, and Cellebrite UFED 4PC.

You can install a standalone installation of the required SafeNet drivers. This enables administrators to use the Admin Control Center and monitor network dongle events without the need to install Cellebrite applications.

To install the SafeNet drivers:

1. Go to http://www.safenet-inc.com/sentineldownloads/#
2. Click **Sentinel HASP/LDK - Windows GUI Run-time Installer**
3. Follow the on-screen instructions.

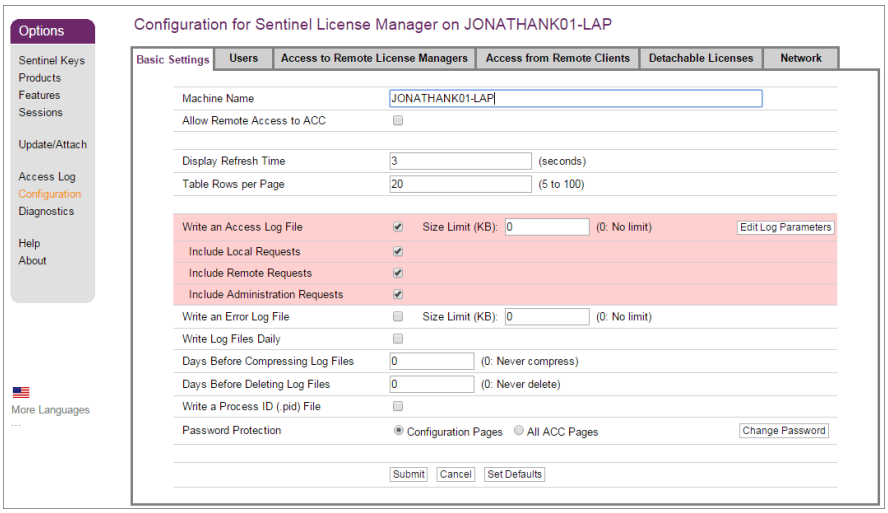
11.21.7. Enabling network dongle logs

The log files are not enabled by default and need to be enabled from within Admin Control Center

The log files need be enabled on the machine where the dongle is installed.

To enable the log file:

1. In the Admin Control Center, click **Configuration** > **Basic Settings**. The following window appears.



For more information to configure basic settings and define access log parameters, click **Help** to display the Help for this page.

2. Select the log file setting check boxes as indicated above.

The log file is stored in the following path:

`C:\Program Files (x86)\Common Files\Aladdin Shared\HASP\`

File name: *Access.log*

Sample:

```
2015-03-04 11:04:00 127.0.0.1:51183 Techlab@WIN-TI4FQ212NGH POST /api/loginex LOGIN_EX
(lm=local,haspid=659816198,productid=0,feat=0,sess=00000002) result(0)
2015-03-04 11:04:01 ::1:51166 [ACC]@::1 GET /_int_/cdata.txt GUI() result(0)
2015-03-04 11:04:03 ::1:51166 [ACC]@::1 GET /_int_/log.html GUI() result(0)
2015-03-04 11:04:03 ::1:51166 [ACC]@::1 GET /_int_/tab_log.html GUI() result(0)
2015-03-04 11:04:06 ::1:51166 [ACC]@::1 GET /_int_/tab_log.html GUI() result(0)
2015-03-04 11:04:09 ::1:51166 [ACC]@::1 GET /_int_/tab_log.html GUI() result(0)
. . .
2015-03-04 11:04:43 127.0.0.1:51185 Techlab@WIN-TI4FQ212NGH POST /api/logout LOGOUT
(lm=local,haspid=659816198,productid=0,feat=0,sess=00000002,duration=43) result(0)
2015-03-04 11:04:44 ::1:51166 [ACC]@::1 GET /_int_/tab_log.html GUI() result(0)
```

In the sample above, you can see the following:

- Date & time: 2015-03-04 11:04:00
- IP address & Port: 127.0.0.1:51183
- By username & machine name: Techlab@WIN-TI4FQ212NGH
- Ask for method: LOGIN
- From license manger: lm=local
- Asked for HASP ID: haspid=659816198
- For feature and product details: productid=0,feat=0
- Created a new session between the protected application and the license: sess=00000002
- And the whole task result is: result(0) (Result 0 = OK)

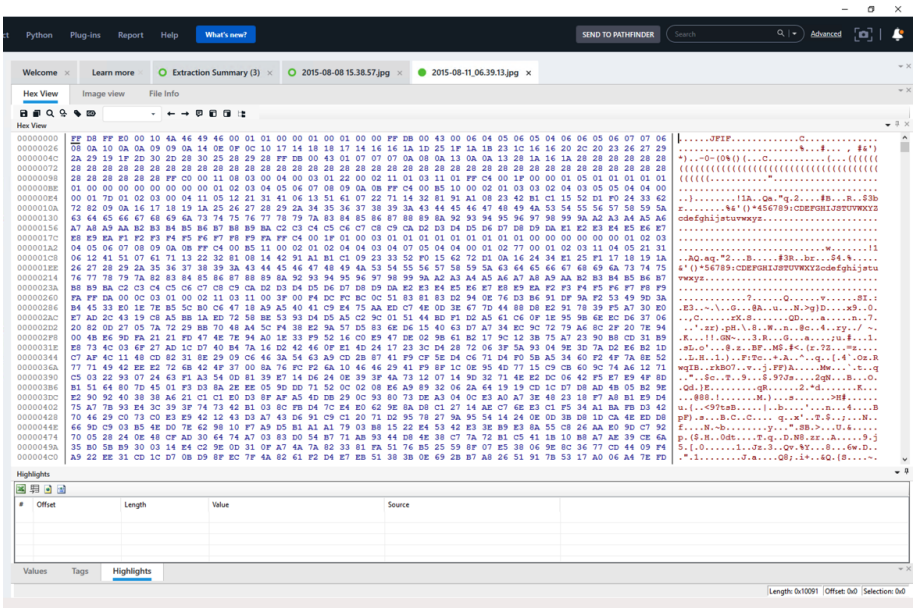
12. Working with hex data

The extraction enables you to view the device image, which is a single file or multiple files that contain a comprehensive copy of the contents and structure of the data on the device.

To access the hex view of the device image:

» In the project tree, expand the **Images** tree item, and double-click the desired image.

An Image tab appears in the data display area showing the image data in Hex view.



Located under the Hex view tab are Analysis Information tabs that display the following types of information related directly to the displayed Hex data:

» **Values** - A wide array of value interpretations, such as 8, 16, 32, and 64 bit, various string encoding, date & time formats, and more, calculated on the fly for the currently selected data in the Hex view. See Working in the Values tab (on page 118).

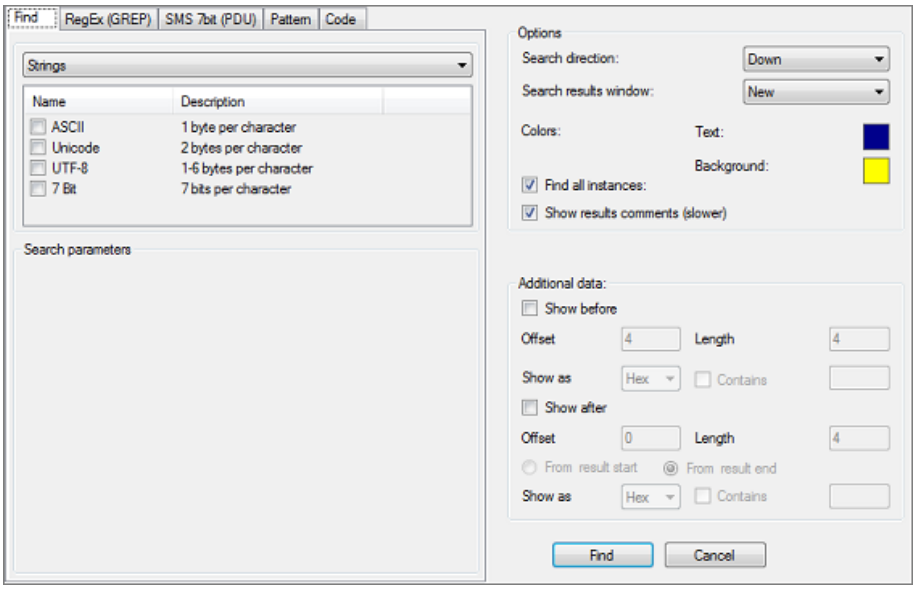
» **Tags**- A list of tags added in the displayed Hex data. See Working with Hex tags (on page 398).

» **Highlights** - A list of content segments markups highlighted in the displayed Hex data. The number of highlight results is shown in brackets next to the tab name. See Working in the Highlights tab (on page 119).

» **Search** - Displays results of a search in the displayed Hex data. A new search results tab opens for each search query performed. The number of results for each search is shown in brackets next to the tab name.

For more information on the Image tab, see Hex view (on page 116).

12.1. Searching for information in the Hex data and decoded data



The Find window has several tabs that enable you to search the Hex data in the following modes:

- **Find** - Search for specific parameters, such as strings, bytes, dates, and more.

> You can search using wild cards: ? and * (? replaces an octet (4 bit) and * replaces an entire byte). There must be an even number of digits before, between or after an asterisk.

- **RegEx (GREP)** - Search for strings using Regular Expressions.
- **SMS 7Bit (PDU)** - Search for SMS text strings.
- **Pattern** - Search for text patterns, in cases in which the pattern of the text is understood but not the text itself (mainly used for 7 bit search to locate SMS messages).
- **Code** - Specialized search for user codes and passwords.

> The **Find** modes were built using the Plug-ins architecture. The find options can be enhanced and extended by adding new search plug-ins.

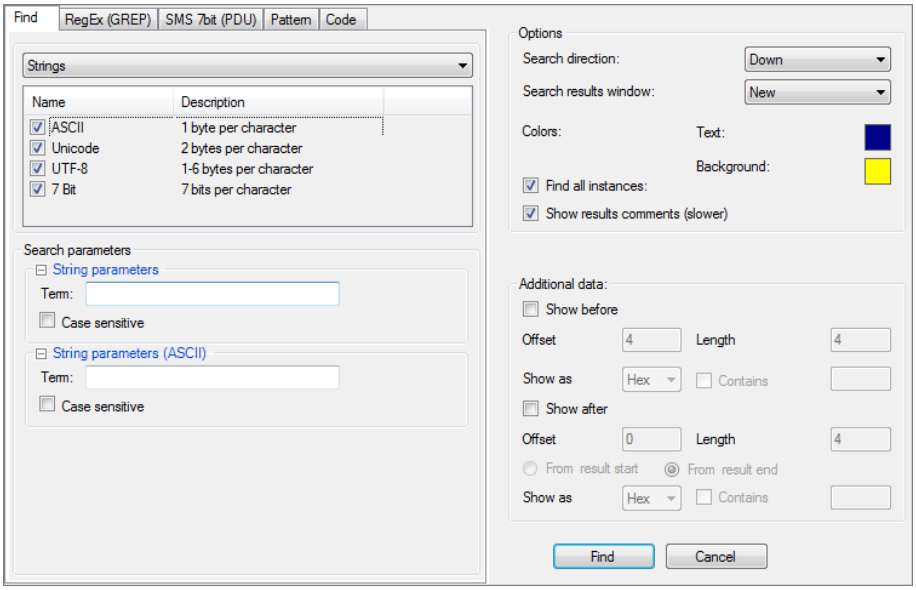
For more information on targeted searches, refer to the following sections:

- Searching strings (below)
- Searching bytes (on page 379)
- Searching dates (on page 381)
- Searching SIM ICCID numbers (on page 384)
- Searching SMS numbers (on page 386)
- Searching for regular expressions (GREP) (on page 388)
- Searching SMS text strings (on page 391)
- Searching for patterns (on page 393)
- Searching for codes and passwords (on page 396)

12.1.1. Searching strings

Search for strings to locate different types of data in the Hex data, e.g. text messages, phone numbers, names or any other string data.

1. While viewing Hex data, click to open the Find window.
2. In the **Find** tab, select **Strings** from the data type list.



3. Select the type of text encoding to search for the given string:
   - ASCII
   - **UNICODE** (mainly for non-Latin characters)
   - UTF-8
   - **7 bits** (mainly for SMS text)

   The **Search parameters** area appears.
4. In the **Search parameters** area:
   a. In the **Term** box in the **String parameters** area, enter the search string.
   b. Select the **Case sensitive** option, if necessary.

5. In the **Options** area, set the desired search options:
   a. In the **Search direction** list, select the search direction.
   b. In the **Search results** window list, select **New**, **Replace current**, or **Add to current**, as desired.
   c. To set the **Text** and **Background** colors, click the color box, select the desired color, and click **OK**.

      The colors you set here are retained for the duration of this session. To change the default colors, set the colors in the Setting window. For more information, see Hex viewer (on page 432).

      Tip: To easily distinguish between the given results of each search performed, set different text and background colors for each search you run.
   d. Do one of the following:
      - Select **Find all instances** to display all search results at the end of the process
      - Clear **Find all instances** to move through the found items one-by-one during the search (can also be done by pressing F3).
   e. Select **Show results comments** to display
6. In the **Additional data** area, enhance your search capabilities by including a predefined number of characters before and/or after the searched value. This can help you locate specific results, or even limit the results to specific entities of the searched value.
   a. Select **Show before** to show the data immediately before what you are searching for.
   b. In the **Offset** box, enter the offset from the start of the search result from which to start including the additional data.
   c. In the **Length** box, enter the length of the additional data to include starting at the set offset point. For **Show before**, the **Length** cannot be longer than the **Offset**.
   d. In the **Show as** box, enter the data type for the additional data to be displayed (**Hex**, **ASCII**, **Unicode**, or **7Bit**).
   e. Select **Contains**, and enter a string that the search result must contain in its additional data.
   f. Select **Show after** to show the data immediately after what you are searching for, and repeat steps 2-5.
   g. For the **Show after** option, set whether the offset and length of the additional data are calculated **From result start** or **From result end**.

   The additional data is logged to the **Additional before** and **Additional after** fields of search results.
7. Click **Find**.

   If you selected **Find All Instances** in the **Options** area, the results appear in the **Search** results tab in the analysis information tab (in the Hex view tab).

   If you did not select **Find All Instances** in the **Options** area, the next found instance is highlighted in the Hex View tab.

The **Search** results tab includes the following:

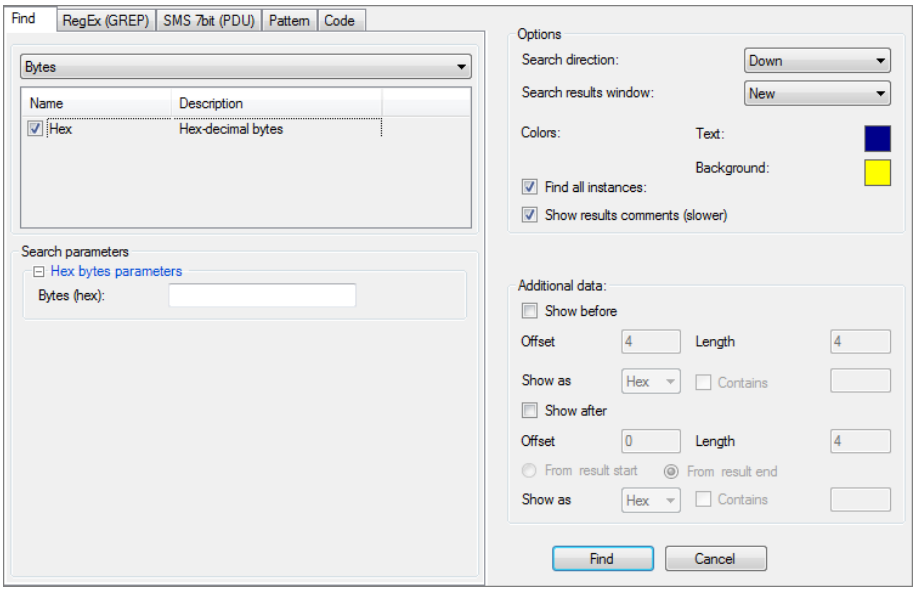
- **#** - The instance number.
- **Offset** - The address offset of the data file in the Hex data.
- **Length** - The string length in bytes.
- **Value** - The string itself.
- **Source**
- **More**
- **Additional before** - If you set additional data options in the Find window, displays the data located immediately before the result.
- **Additional after** - If you set additional data options in the Find window, displays the data located immediately after the result.

8. To display a result instance in the Hex view tab, click on the desired row in the search results tab.
9. To search for specific data and filter the search results, use the **Find** box in the search results tab.
10. To export the search results list, click the desired output in the **Search** tab toolbar: Excel , HTML , PDF , or XML .

12.1.2. Searching bytes

Search for bytes to look for specific occurrences in the Hex data. This is especially useful when you know the identifying header of a file type or information you are looking for. For example, the starting Hex bytes of a jpeg image are **FF D8 FF**. Therefore, the result of searching for **FF D8 FF** provides the locations of all possible jpeg image headers in the Hex data.

1. While viewing Hex data, click to open the Find window.
2. In the **Find** tab, select **Bytes** from the data type list.



3. Select **Hex**.

   The **Search parameters** area appears.

4. In the **Bytes (hex)** box, enter the Hex value, for example, **FFD8FF**.
5. In the **Options** area, set the desired search options:
   a. In the **Search direction** list, select the search direction.
   b. In the **Search results** window list, select **New**, **Replace current**, or **Add to current**, as desired.
   c. To set the **Text** and **Background** colors, click the color box, select the desired color, and click **OK**.

      The colors you set here are retained for the duration of this session. To change the default colors, set the colors in the Setting window. For more information, see Hex viewer (on page 432).

      Tip: To easily distinguish between the given results of each search performed, set different text and background colors for each search you run.
   d. Do one of the following:
      - Select **Find all instances** to display all search results at the end of the process
      - Clear **Find all instances** to move through the found items one-by-one during the search (can also be done by pressing F3).
   e. Select **Show results comments** to display
6. In the **Additional data** area, enhance your search capabilities by including a predefined number of characters before and/or after the searched value. This can help you locate specific results, or even limit the results to specific entities of the searched value.
   a. Select **Show before** to show the data immediately before what you are searching for.
   b. In the **Offset** box, enter the offset from the start of the search result from which to start including the additional data.
   c. In the **Length** box, enter the length of the additional data to include starting at the set offset point. For **Show before**, the **Length** cannot be longer than the **Offset**.
   d. In the **Show as** box, enter the data type for the additional data to be displayed (**Hex**, **ASCII**, **Unicode**, or **7Bit**).
   e. Select **Contains**, and enter a string that the search result must contain in its additional data.
   f. Select **Show after** to show the data immediately after what you are searching for, and repeat steps 2-5.
   g. For the **Show after** option, set whether the offset and length of the additional data are calculated **From result start** or **From result end**.

   The additional data is logged to the **Additional before** and **Additional after** fields of search results.

7. Click **Find**.

   If you selected **Find All Instances** in the **Options** area, the results appear in the **Search results** tab in the analysis information tab (in the Hex view tab).

If you did not select **Find All Instances** in the **Options** area, the next found instance is highlighted in the Hex View tab.

The **Search** results tab includes the following:

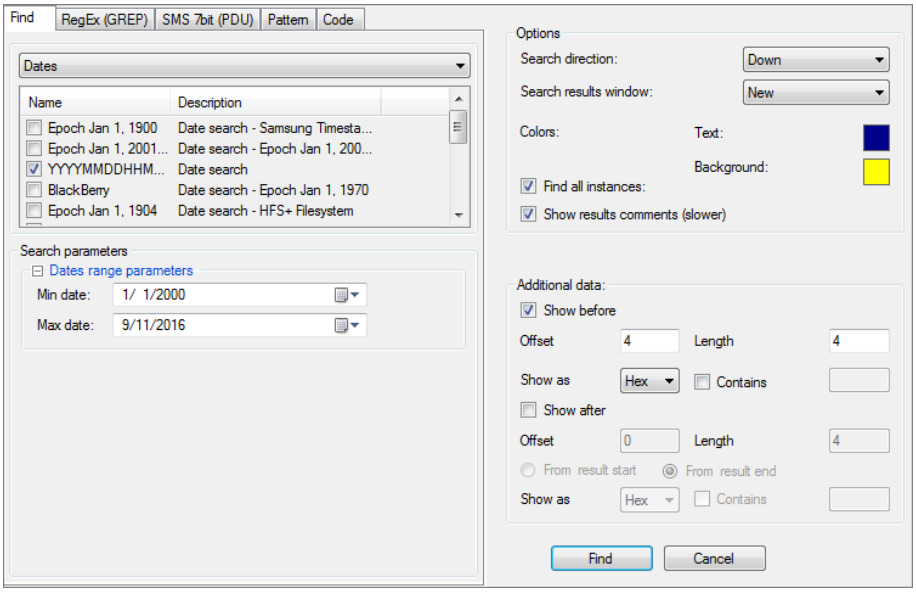
- **#** - The instance number.
- **Offset** - The address offset of the data file in the Hex data.
- **Length** - The string length in bytes.
- **Value** - The string itself.
- **Source**
- **More**
- **Additional before** - If you set additional data options in the Find window, displays the data located immediately before the result.
- **Additional after** - If you set additional data options in the Find window, displays the data located immediately after the result.

8. To display a result instance in the Hex view tab, click on the desired row in the search results tab.
9. To search for specific data and filter the search results, use the **Find** box in the search results tab.
10. To export the search results list, click the desired output in the **Search** tab toolbar: Excel , HTML , PDF , or XML .

12.1.3. Searching dates

Search for dates to find date ranges in the Hex data.

1. While viewing Hex data, click to open the Find window.
2. In the **Find** tab, select **Dates** from the data type list.



The filter box displays a list of date formats and plug-ins that can be used for date searches.

3. Select the desired date format(s) and any plug-in(s) that you want to use in the current search.

> What plug-ins are suitable depends on how the data is encoded, what type of device you are analyzing, and so on. If you select a plug-in that is not suitable, your search results may contain false results. For example, you can select **BlackBerry** if you are analyzing a BlackBerry device. If you are not analyzing a BlackBerry device, selecting **BlackBerry** may return results that are inaccurate.

The **Search parameters** area appears.

4. In the **Min Date** and **Max Date** fields, click to select a date from the calendar.

   Tip: Set a short date range in order to reduce the number of given results.

   Tip: When searching for a particular date, set the **Min Date** and **Max Date** fields to a range of no more than 24 hours.

5. In the **Options** area, set the desired search options:
   a. In the **Search direction** list, select the search direction.
   b. In the **Search results** window list, select **New**, **Replace current**, or **Add to current**, as desired.
   c. To set the **Text** and **Background** colors, click the color box, select the desired color, and click **OK**.

      The colors you set here are retained for the duration of this session. To change the default colors, set the colors in the Setting window. For more information, see Hex viewer (on page 432).

      Tip: To easily distinguish between the given results of each search performed, set different text and background colors for each search you run.
   d. Do one of the following:
      - Select **Find all instances** to display all search results at the end of the process.
      - Clear **Find all instances** to move through the found items one-by-one during the search (can also be done by pressing F3).
   e. Select **Show results comments** to display.

6. In the **Additional data** area, enhance your search capabilities by including a predefined number of characters before and/or after the searched value. This can help you locate specific results, or even limit the results to specific entities of the searched value.
   a. Select **Show before** to show the data immediately before what you are searching for.
   b. In the **Offset** box, enter the offset from the start of the search result from which to start including the additional data.
   c. In the **Length** box, enter the length of the additional data to include starting at the set offset point. For **Show before**, the **Length** cannot be longer than the **Offset**.
   d. In the **Show as** box, enter the data type for the additional data to be displayed (**Hex**, **ASCII**, **Unicode**, or **7Bit**).
   e. Select **Contains**, and enter a string that the search result must contain in its additional data.
   f. Select **Show after** to show the data immediately after what you are searching for, and repeat steps 2-5.
   g. For the **Show after** option, set whether the offset and length of the additional data are calculated **From result start** or **From result end**.

   The additional data is logged to the **Additional before** and **Additional after** fields of search results.
7. Click **Find**.

   If you selected **Find All Instances** in the **Options** area, the results appear in the **Search** results tab in the analysis information tab (in the Hex view tab).

   If you did not select **Find All Instances** in the **Options** area, the next found instance is highlighted in the Hex View tab.

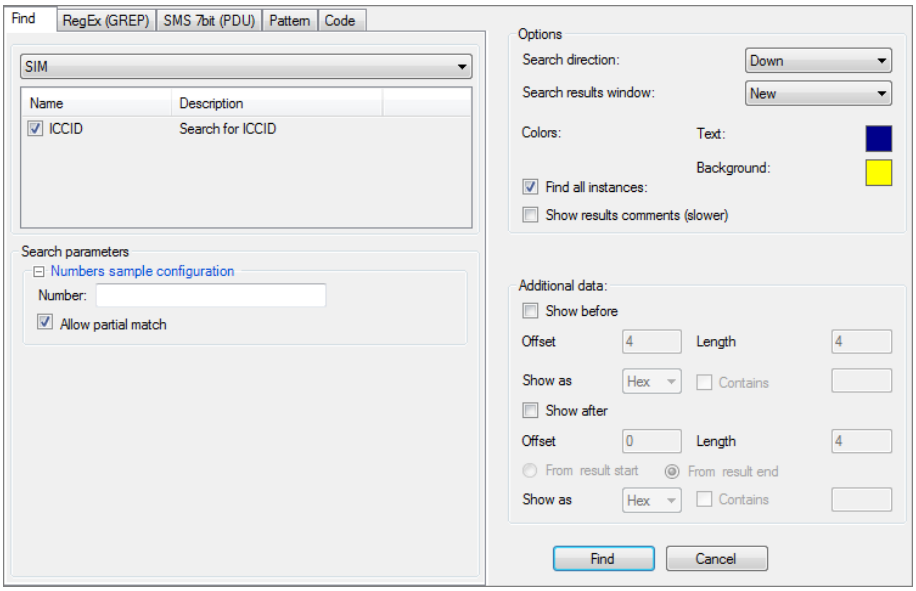
   The **Search** results tab includes the following:

   - **#** - The instance number.
   - **Offset** - The address offset of the data file in the Hex data.
   - **Length** - The string length in bytes.
   - **Value** - The string itself.
   - **Source**
   - **More**
   - **Additional before** - If you set additional data options in the Find window, displays the data located immediately before the result.
   - **Additional after** - If you set additional data options in the Find window, displays the data located immediately after the result.
8. To display a result instance in the Hex view tab, click on the desired row in the search results tab.
9. To search for specific data and filter the search results, use the **Find** box in the search results tab.
10. To export the search results list, click the desired output in the **Search** tab toolbar: Excel , HTML , PDF , or XML .

12.1.4. Searching SIM ICCID numbers

This search method enables you to search for SIM ICCID numbers in the Hex data.

1. While viewing Hex data, click to open the Find window.
2. In the **Find** tab, select **SIM** from the data type list.



3. Select **ICCID**.

   The **Search parameters** area appears.
4. In the Numbers sample configuration area, enter the ICCID number in the **Number** box.
5. If you entered only part of the number, select **Allow Partial Match**. For example, entering the number **89972** and selecting this option, Physical Analyzer searches for ICCID numbers provided by a service provider.
6. In the **Options** area, set the desired search options:
   a. In the **Search direction** list, select the search direction.
   b. In the **Search results** window list, select **New**, **Replace current**, or **Add to current**, as desired.
   c. To set the **Text** and **Background** colors, click the color box, select the desired color, and click **OK**.

      The colors you set here are retained for the duration of this session. To change the default colors, set the colors in the Setting window. For more information, see Hex viewer (on page 432).

      Tip: To easily distinguish between the given results of each search performed, set different text and background colors for each search you run.

d. Do one of the following:
   - Select **Find all instances** to display all search results at the end of the process
   - Clear **Find all instances** to move through the found items one-by-one during the search (can also be done by pressing F3).

e. Select **Show results comments** to display

7. In the **Additional data** area, enhance your search capabilities by including a predefined number of characters before and/or after the searched value. This can help you locate specific results, or even limit the results to specific entities of the searched value.
   a. Select **Show before** to show the data immediately before what you are searching for.
   b. In the **Offset** box, enter the offset from the start of the search result from which to start including the additional data.
   c. In the **Length** box, enter the length of the additional data to include starting at the set offset point. For **Show before**, the **Length** cannot be longer than the **Offset**.
   d. In the **Show as** box, enter the data type for the additional data to be displayed (**Hex**, **ASCII**, **Unicode**, or **7Bit**).
   e. Select **Contains**, and enter a string that the search result must contain in its additional data.
   f. Select **Show after** to show the data immediately after what you are searching for, and repeat steps 2-5.
   g. For the **Show after** option, set whether the offset and length of the additional data are calculated **From result start** or **From result end**.

   The additional data is logged to the **Additional before** and **Additional after** fields of search results.

8. Click **Find**.

> If the **Number** field is left empty, the search results include all the numbers that match the ICCID format.

If you selected **Find All Instances** in the **Options** area, the results appear in the **Search** results tab in the analysis information tab (in the Hex view tab).

If you did not select **Find All Instances** in the **Options** area, the next found instance is highlighted in the Hex View tab.

The **Search** results tab includes the following:

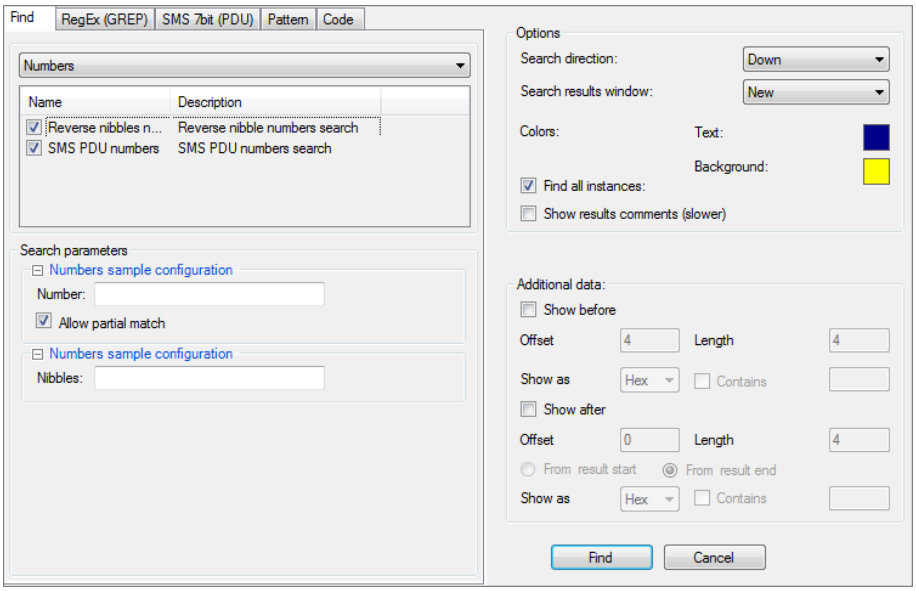
- **#** - The instance number.
- **Offset** - The address offset of the data file in the Hex data.
- **Length** - The string length in bytes.
- **Value** - The string itself.
- Source
- More
- **Additional before** - If you set additional data options in the Find window, displays the data located immediately before the result.
- **Additional after** - If you set additional data options in the Find window, displays the data located immediately after the result.

9. To display a result instance in the Hex view tab, click on the desired row in the search results tab.
10. To search for specific data and filter the search results, use the **Find** box in the search results tab.
11. To export the search results list, click the desired output in the **Search** tab toolbar: Excel , HTML , PDF , or XML .

12.1.5. Searching SMS numbers

Search for SMS numbers in the Hex data.

1. While viewing Hex data, click to open the Find window.
2. In the **Find** tab, select **Numbers** from the data type list.



3. To perform a search of SMS PDU numbers, select **SMS PDU numbers**.

   The **Search parameters** area appears.

a. In the **Number** field, enter the search number.

> If the **Number** field is left empty, the search results include all the numbers that match the SMS Number format.

b. If you entered only part of the number, select **Allow Partial Match**.

4. To a search for reversed nibbles, select **Reverse nibbles numbers**.

> Use this option when the data has been encoded to include reversed nibbles.

The **Search parameters** area appears.

» In the **Nibbles** field, enter the desired nibble.

5. In the **Options** area, set the desired search options:
   a. In the **Search direction** list, select the search direction.
   b. In the **Search results** window list, select **New**, **Replace current**, or **Add to current**, as desired.
   c. To set the **Text** and **Background** colors, click the color box, select the desired color, and click **OK**.

      The colors you set here are retained for the duration of this session. To change the default colors, set the colors in the Setting window. For more information, see Hex viewer (on page 432).

      Tip: To easily distinguish between the given results of each search performed, set different text and background colors for each search you run.
   d. Do one of the following:
      » Select **Find all instances** to display all search results at the end of the process
      » Clear **Find all instances** to move through the found items one-by-one during the search (can also be done by pressing F3).
   e. Select **Show results comments** to display
6. In the **Additional data** area, enhance your search capabilities by including a predefined number of characters before and/or after the searched value. This can help you locate specific results, or even limit the results to specific entities of the searched value.
   a. Select **Show before** to show the data immediately before what you are searching for.
   b. In the **Offset** box, enter the offset from the start of the search result from which to start including the additional data.
   c. In the **Length** box, enter the length of the additional data to include starting at the set offset point. For **Show before**, the **Length** cannot be longer than the **Offset**.
   d. In the **Show as** box, enter the data type for the additional data to be displayed (**Hex**, **ASCII**, **Unicode**, or **7Bit**).

e. Select **Contains**, and enter a string that the search result must contain in its additional data.

f. Select **Show after** to show the data immediately after what you are searching for, and repeat steps 2-5.

g. For the **Show after** option, set whether the offset and length of the additional data are calculated **From result start** or **From result end**.

The additional data is logged to the **Additional before** and **Additional after** fields of search results.

7. Click **Find**.

   If you selected **Find All Instances** in the **Options** area, the results appear in the **Search** results tab in the analysis information tab (in the Hex view tab).

   If you did not select **Find All Instances** in the **Options** area, the next found instance is highlighted in the Hex View tab.

   The **Search** results tab includes the following:

   - **#** - The instance number.
   - **Offset** - The address offset of the data file in the Hex data.
   - **Length** - The string length in bytes.
   - **Value** - The string itself.
   - **Source**
   - **More**
   - **Additional before** - If you set additional data options in the Find window, displays the data located immediately before the result.
   - **Additional after** - If you set additional data options in the Find window, displays the data located immediately after the result.

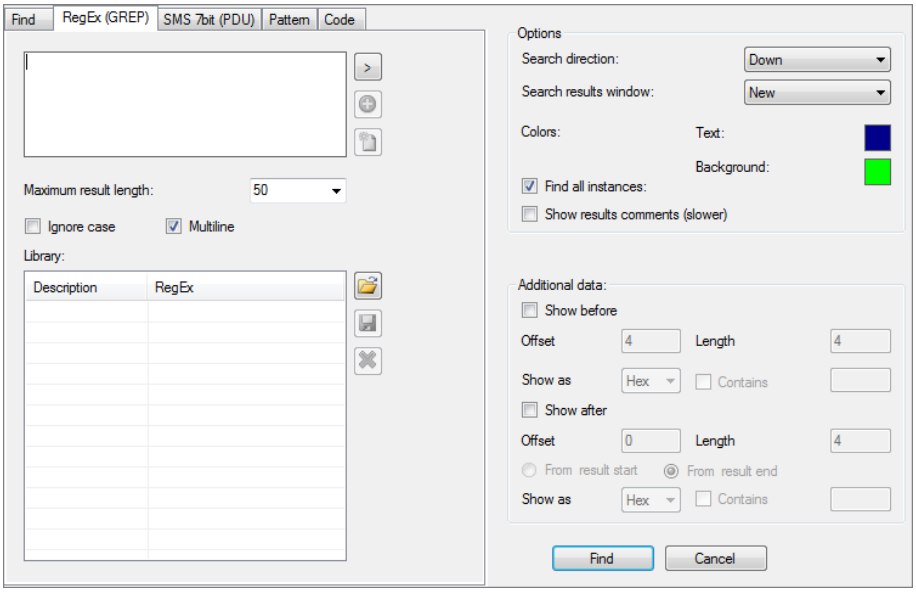
8. To display a result instance in the Hex view tab, click on the desired row in the search results tab.
9. To search for specific data and filter the search results, use the **Find** box in the search results tab.
10. To export the search results list, click the desired output in the **Search** tab toolbar: Excel , HTML , PDF , or XML .

12.1.6. Searching for regular expressions (GREP)

Search for regular expressions to (RegEx) in order to look for a specific string structure within the data.

For example, the regular expression "**[a-zA-Z0-9._%+-]+@[a-zA-Z0-9.-]+\.[A-Za-z]{2,4}**", Physical Analyzer searches your data for all the email addresses that match the structure **<string>@<string>.<2 to 4 letters>**.

1. While viewing Hex data, click to open the Find window.



2. In the **RegEx (GREP)** tab, enter the expression that you want to use in the search.
3. Click to enter a regular expression code from a list of common codes.
4. Click to save the current expression in the library list.
5. Click to clear the regular expression field.
6. Set the **Maximum result length** value to filter only results that are up to the specified length.
7. Select **Ignore case** to disregard the case in the search results.
8. Select **Multiline**.
9. To use a saved expression from the library, click it in the **Library** area.
10. To export the current regular expression library to a *.rel file, click .
11. To load an exported regular expression from a *.rel file, click .
12. To delete an expression from the library list, click .
13. In the **Options** area, set the desired search options:
    a. In the **Search direction** list, select the search direction.
    b. In the **Search results** window list, select **New**, **Replace current**, or **Add to current**, as desired.
    c. To set the **Text** and **Background** colors, click the color box, select the desired color, and click **OK**.

    The colors you set here are retained for the duration of this session. To change the default colors, set the colors in the Setting window. For more information, see Hex viewer (on page 432).

    Tip: To easily distinguish between the given results of each search performed, set different text and background colors for each search you run.

d. Do one of the following:
   - Select **Find all instances** to display all search results at the end of the process
   - Clear **Find all instances** to move through the found items one-by-one during the search (can also be done by pressing F3).

e. Select **Show results comments** to display

14. In the **Additional data** area, enhance your search capabilities by including a predefined number of characters before and/or after the searched value. This can help you locate specific results, or even limit the results to specific entities of the searched value.

    a. Select **Show before** to show the data immediately before what you are searching for.

    b. In the **Offset** box, enter the offset from the start of the search result from which to start including the additional data.

    c. In the **Length** box, enter the length of the additional data to include starting at the set offset point. For **Show before**, the **Length** cannot be longer than the **Offset**.

    d. In the **Show as** box, enter the data type for the additional data to be displayed (**Hex**, **ASCII**, **Unicode**, or **7Bit**).

    e. Select **Contains**, and enter a string that the search result must contain in its additional data.

    f. Select **Show after** to show the data immediately after what you are searching for, and repeat steps 2-5.

    g. For the **Show after** option, set whether the offset and length of the additional data are calculated **From result start** or **From result end**.

    The additional data is logged to the **Additional before** and **Additional after** fields of search results.

15. Click **Find**.

    If you selected **Find All Instances** in the **Options** area, the results appear in the **Search** results tab in the analysis information tab (in the Hex view tab).

    If you did not select **Find All Instances** in the **Options** area, the next found instance is highlighted in the Hex View tab.

    The **Search** results tab includes the following:

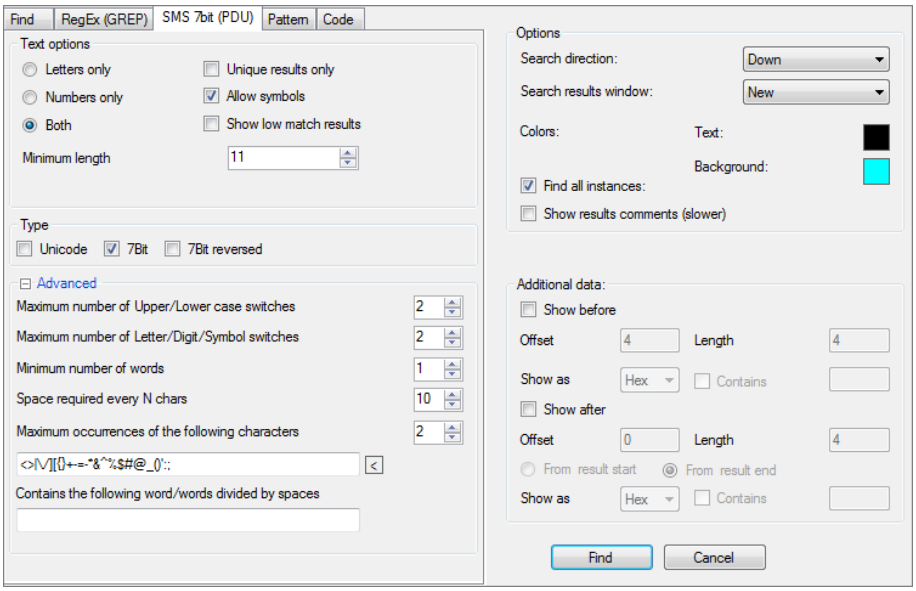
    - **#** - The instance number.
    - **Offset** - The address offset of the data file in the Hex data.
    - **Length** - The string length in bytes.
    - **Value** - The string itself.
    - **Source**
    - **More**
    - **Additional before** - If you set additional data options in the Find window, displays the data located immediately before the result.
    - **Additional after** - If you set additional data options in the Find window, displays the data located immediately after the result.

16. To display a result instance in the Hex view tab, click on the desired row in the search results tab.
17. To search for specific data and filter the search results, use the **Find** box in the search results tab.
18. To export the search results list, click the desired output in the **Search** tab toolbar: Excel, HTML, PDF, or XML.

12.1.7. Searching SMS text strings

This search method enables you to search for SMS text strings (7bit PDU) in the Hex data

1. While viewing Hex data, click to open the Find window.
2. Select the **SMS 7Bit (PDU)** tab.



3. In the **Text Options** area, set the following search parameters:
   a. Set the search type: **Letters only**, **Numbers only**, or **Both**.
   b. To show unique results, select **Unique results only**.
   c. To allow symbols in the search results, select **Allow symbols**.
   d. To show low match results, select **Show low match results**.
   e. To set the minimum number of characters in the results, set the **Minimum length**.
4. In the **Type** area, select the search type: **Unicode**, **7Bit**, **7Bit reversed**.
5. In the **Advanced** area, set the following, as applicable:
   - Maximum number of Upper/Lower case switches
   - Maximum number of Letter/Digit/Symbol switches
   - Minimum number of words
   - Space required every N chars
   - Maximum occurrences of the following characters
   - Contains the following words divided by spaces.

6. In the **Options** area, set the desired search options:
   a. In the **Search direction** list, select the search direction.
   b. In the **Search results** window list, select **New**, **Replace current**, or **Add to current**, as desired.
   c. To set the **Text** and **Background** colors, click the color box, select the desired color, and click **OK**.

      The colors you set here are retained for the duration of this session. To change the default colors, set the colors in the Setting window. For more information, see Hex viewer (on page 432).

      Tip: To easily distinguish between the given results of each search performed, set different text and background colors for each search you run.
   d. Do one of the following:
      - Select **Find all instances** to display all search results at the end of the process
      - Clear **Find all instances** to move through the found items one-by-one during the search (can also be done by pressing F3).
   e. Select **Show results comments** to display
7. In the **Additional data** area, enhance your search capabilities by including a predefined number of characters before and/or after the searched value. This can help you locate specific results, or even limit the results to specific entities of the searched value.
   a. Select **Show before** to show the data immediately before what you are searching for.
   b. In the **Offset** box, enter the offset from the start of the search result from which to start including the additional data.
   c. In the **Length** box, enter the length of the additional data to include starting at the set offset point. For **Show before**, the **Length** cannot be longer than the **Offset**.
   d. In the **Show as** box, enter the data type for the additional data to be displayed (**Hex**, **ASCII**, **Unicode**, or **7Bit**).
   e. Select **Contains**, and enter a string that the search result must contain in its additional data.
   f. Select **Show after** to show the data immediately after what you are searching for, and repeat steps 2-5.
   g. For the **Show after** option, set whether the offset and length of the additional data are calculated **From result start** or **From result end**.

   The additional data is logged to the **Additional before** and **Additional after** fields of search results.
8. Click **Find**.

   If you selected **Find All Instances** in the **Options** area, the results appear in the **Search** results tab in the analysis information tab (in the Hex view tab).

   If you did not select **Find All Instances** in the **Options** area, the next found instance is highlighted in the Hex View tab.

   The **Search** results tab includes the following:

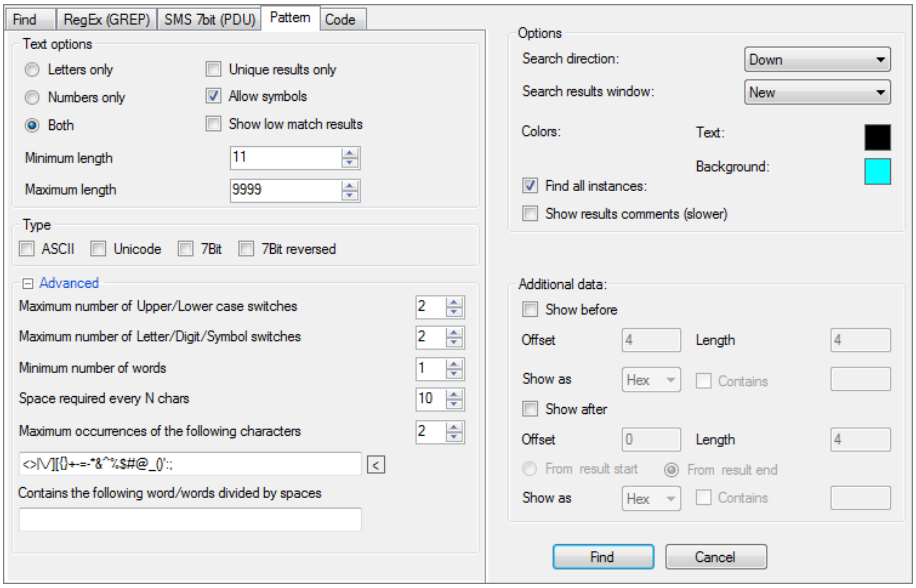
- **#** - The instance number.
- **Offset** - The address offset of the data file in the Hex data.
- **Length** - The string length in bytes.
- **Value** - The string itself.
- **Source**
- **More**
- **Additional before** - If you set additional data options in the Find window, displays the data located immediately before the result.
- **Additional after** - If you set additional data options in the Find window, displays the data located immediately after the result.

9. To display a result instance in the Hex view tab, click on the desired row in the search results tab.
10. To search for specific data and filter the search results, use the **Find** box in the search results tab.
11. To export the search results list, click the desired output in the **Search** tab toolbar: Excel, HTML, PDF, or XML.

12.1.8. Searching for patterns

When navigating within a large memory structure, the search for patterns to locate any content that is textual in nature.

1. While viewing Hex data, click to open the Find window.
2. Select the **Pattern** tab.



3. In the **Text Options** area, set the following search parameters:
   a. Set the search type: **Letters only**, **Numbers only**, or **Both**.
   b. To show unique results, select **Unique results only**.
   c. To allow symbols in the search results, select **Allow symbols**.
   d. To show low match results, select **Show low match results**.
4. In the **Minimal length** and **Maximal length** fields, set the pattern length range.

   This option enables you to filter the results according to the searched patterns.
5. In the **Type** area, select the search type: **ASCII**, **Unicode**, **7Bit** and/or **7Bit reversed**.
6. In the **Advanced** area, set the following, as applicable:
   - Maximum number of Upper/Lower case switches
   - Maximum number of Letter/Digit/Symbol switches
   - Minimum number of words
   - Space required every N chars
   - Maximum occurrences of the following characters
   - Contains the following words divided by spaces.
7. In the **Options** area, set the desired search options:
   a. In the **Search direction** list, select the search direction.
   b. In the **Search results** window list, select **New**, **Replace current**, or **Add to current**, as desired.
   c. To set the **Text** and **Background** colors, click the color box, select the desired color, and click **OK**.

      The colors you set here are retained for the duration of this session. To change the default colors, set the colors in the Setting window. For more information, see Hex viewer (on page 432).

      Tip: To easily distinguish between the given results of each search performed, set different text and background colors for each search you run.
   d. Do one of the following:
      - Select **Find all instances** to display all search results at the end of the process
      - Clear **Find all instances** to move through the found items one-by-one during the search (can also be done by pressing F3).
   e. Select **Show results comments** to display
8. In the **Additional data** area, enhance your search capabilities by including a predefined number of characters before and/or after the searched value. This can help you locate specific results, or even limit the results to specific entities of the searched value.
   a. Select **Show before** to show the data immediately before what you are searching for.
   b. In the **Offset** box, enter the offset from the start of the search result from which to start including the additional data.
   c. In the **Length** box, enter the length of the additional data to include starting at the set offset point. For **Show before**, the **Length** cannot be longer than the **Offset**.

d. In the **Show as** box, enter the data type for the additional data to be displayed (**Hex**, **ASCII**, **Unicode**, or **7Bit**).
e. Select **Contains**, and enter a string that the search result must contain in its additional data.
f. Select **Show after** to show the data immediately after what you are searching for, and repeat steps 2-5.
g. For the **Show after** option, set whether the offset and length of the additional data are calculated **From result start** or **From result end**.

The additional data is logged to the **Additional before** and **Additional after** fields of search results.

9. Click **Find**.

> Pattern search can be used to locate all possible 7 bit SMS text results. To minimize the number of false positive results set the **Minimal Length** value to a higher number.

If you selected **Find All Instances** in the **Options** area, the results appear in the **Search** results tab in the analysis information tab (in the Hex view tab).

If you did not select **Find All Instances** in the **Options** area, the next found instance is highlighted in the Hex View tab.

The **Search** results tab includes the following:

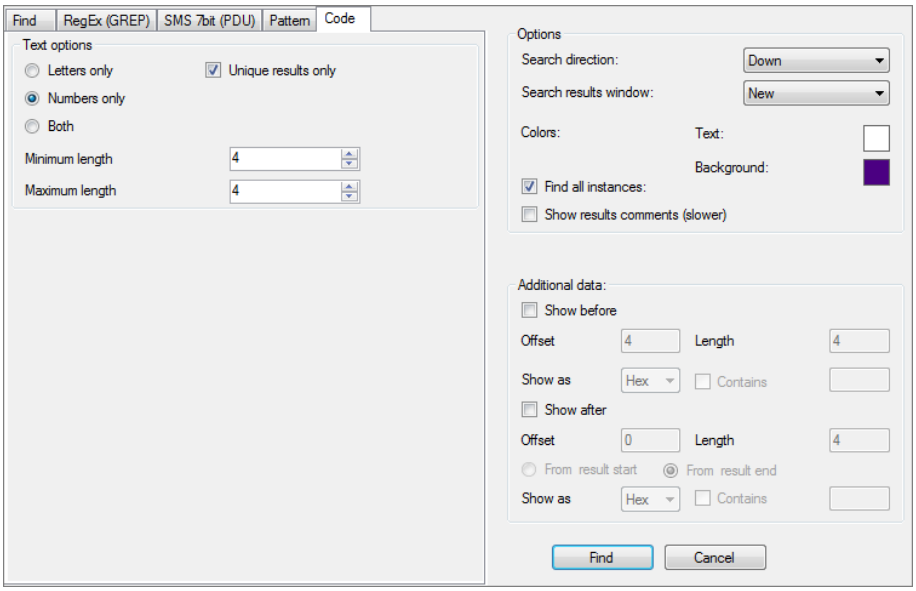
- **#** - The instance number.
- **Offset** - The address offset of the data file in the Hex data.
- **Length** - The string length in bytes.
- **Value** - The string itself.
- **Source**
- **More**
- **Additional before** - If you set additional data options in the Find window, displays the data located immediately before the result.
- **Additional after** - If you set additional data options in the Find window, displays the data located immediately after the result.

10. To display a result instance in the Hex view tab, click on the desired row in the search results tab.
11. To search for specific data and filter the search results, use the **Find** box in the search results tab.
12. To export the search results list, click the desired output in the **Search** tab toolbar: Excel, HTML, PDF, or XML.

12.1.9. Searching for codes and passwords

Search large memory structures for user codes and passwords.

1. While viewing Hex data, click to open the Find window.
2. Select the **Code** tab.



3. In the **Text Options** area, set the following search parameters:
   a. Set the search type: **Letters only**, **Numbers only**, or **Both**.
   b. To show unique results, select **Unique results only**.
4. In the **Minimal length** and **Maximal length** fields, set the pattern length range.

   This option enables you to filter the results according to the searched patterns.
5. In the **Options** area, set the desired search options:
   a. In the **Search direction** list, select the search direction.
   b. In the **Search results** window list, select **New**, **Replace current**, or **Add to current**, as desired.
   c. To set the **Text** and **Background** colors, click the color box, select the desired color, and click **OK**.

      The colors you set here are retained for the duration of this session. To change the default colors, set the colors in the Setting window. For more information, see Hex viewer (on page 432).

      Tip: To easily distinguish between the given results of each search performed, set different text and background colors for each search you run.
   d. Do one of the following:
      - Select **Find all instances** to display all search results at the end of the process
      - Clear **Find all instances** to move through the found items one-by-one during the search (can also be done by pressing F3).
   e. Select **Show results comments** to display

6. In the **Additional data** area, enhance your search capabilities by including a predefined number of characters before and/or after the searched value. This can help you locate specific results, or even limit the results to specific entities of the searched value.
   a. Select **Show before** to show the data immediately before what you are searching for.
   b. In the **Offset** box, enter the offset from the start of the search result from which to start including the additional data.
   c. In the **Length** box, enter the length of the additional data to include starting at the set offset point. For **Show before**, the **Length** cannot be longer than the **Offset**.
   d. In the **Show as** box, enter the data type for the additional data to be displayed (**Hex**, **ASCII**, **Unicode**, or **7Bit**).
   e. Select **Contains**, and enter a string that the search result must contain in its additional data.
   f. Select **Show after** to show the data immediately after what you are searching for, and repeat steps 2-5.
   g. For the **Show after** option, set whether the offset and length of the additional data are calculated **From result start** or **From result end**.

   The additional data is logged to the **Additional before** and **Additional after** fields of search results.
7. Click **Find**.

   If you selected **Find All Instances** in the **Options** area, the results appear in the **Search** results tab in the analysis information tab (in the Hex view tab).

   If you did not select **Find All Instances** in the **Options** area, the next found instance is highlighted in the Hex View tab.

   The **Search** results tab includes the following:

   - **#** - The instance number.
   - **Offset** - The address offset of the data file in the Hex data.
   - **Length** - The string length in bytes.
   - **Value** - The string itself.
   - **Source**
   - **More**
   - **Additional before** - If you set additional data options in the Find window, displays the data located immediately before the result.
   - **Additional after** - If you set additional data options in the Find window, displays the data located immediately after the result.
8. To display a result instance in the Hex view tab, click on the desired row in the search results tab.
9. To search for specific data and filter the search results, use the **Find** box in the search results tab.
10. To export the search results list, click the desired output in the **Search** tab toolbar: Excel , HTML , PDF , or XML .

12.2. Browsing the hex extraction

» Double-click on a binary hex extraction in the project tree to display its content in a Hex view tab in the data display area.

> You can also click the image links in the Extraction Log area at the bottom of the Extraction Summary tab to access the Hex extraction.

12.3. Using an offset to jump to a different location in the file

Scan the Hex data by setting an offset value by which to jump through the data.

To move from a set position:

1. Click GO.
2. Select **Decimal** or **Hex** and in the **Offset** box, enter the offset value in the relevant format.
3. In the **From** area, set the reference point from which to set the offset (**Beginning of file**, **Current position**, or **End of file**).
4. Click **Go**.

   The cursor moves to the offset location.

To move from the current location:

1. Click on a specific location in the Hex data.
2. In the offset value box in the toolbar, enter the desired offset value in decimal format (20) or Hex value format (0x20), or select one of the previously entered values from the list.

   > Type **+** or **-** before the value to calculate the offset from the current position.

3. Do one of the following:
   - » Click ⬅ to jump backwards through the Hex data according to the set value.
   - » Click ➡ to jump forwards through the Hex data according to the set value.

12.4. Working with Hex tags

A Hex tag is a quick reference pointer you can create on Hex data.

The tags you create are managed in the **Hex Tags** tree item. The number of Hex tags in the project is shown in brackets next to the **Hex Tags** tree item.

» In the project tree, double-click **Hex Tags** to list the tags in a tab in the data display area.

» To print or export the Hex tags list, click the desired output in the **Hex Tags** tab toolbar: Excel, HTML, PDF, or XML.

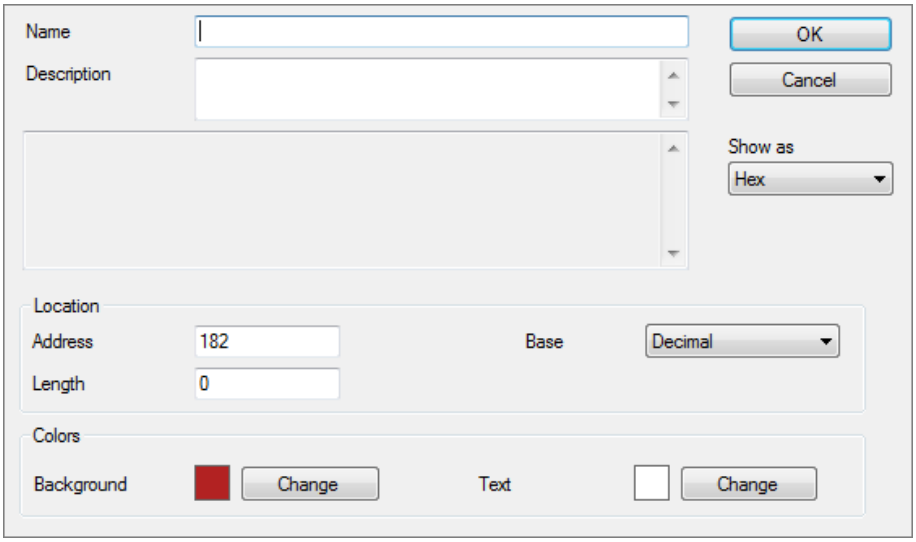
12.4.1. Adding a Hex tag

1. While viewing Hex data, do one of the following:

   » In the **Hex View** tab toolbar, click .

   » To bookmark a specific segment in the Hex data, highlight the section that you want to bookmark, and then click in the Hex View tab toolbar.

   The Add tag dialog box is displayed.



2. In the **Name** box, enter a name for the Hex tag.
3. In the **Description** box, enter a description for the Hex tag.
4. If you did not highlight an area in the Hex, in the **Location** area, do the following:
   a. Select the desired unit for the address, **Decimal** or **Hex**, from the **Base** list.
   b. In the **Address** box, enter the address of the start point (offset) of the data you want to tag.
   c. In the **Length** box, enter the length of the data you want to tag.
5. In the **Colors** area, set the Background and Text colors for the tag.
6. Click **OK**.

   The new Hex tag is saved and displayed in the **Hex tags** tab.

   The marked segment is highlighted in the chosen colors. Details about the Hex tag appear in the results window.

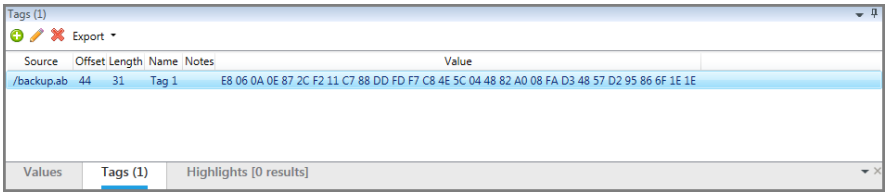
   Each Hex tag displays the following information:

- **Offset** - The address offset of the bookmark paragraph in the Hex data.
- **Length** - The bookmarked data segment length.
- **Description** - The bookmark name.

7. Click on a Hex tag item in the Hex tag list to display it in Hex view.

12.4.2. Editing a Hex tag

1. In the Hex data tab, click the Tag tab. The following tab is displayed.



2. Click to edit an existing tag. The Add tag window appears.
3. Change the tag as desired, and click **OK**.
4. To delete a tag, click .

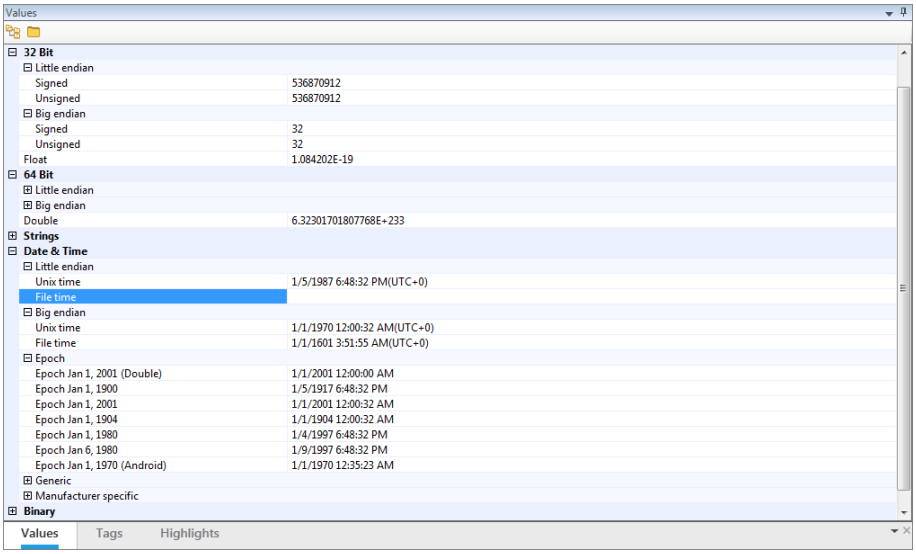
12.5. Decoding raw data

Select segments of the Hex data and decode them to a variety of encoding types on the fly.

Physical Analyzer can decode Hex data to 8 Bit, 16 Bit, 32 Bit, 64 Bit, Strings, Date & Time, Binary, and Numbers.

To decode segments of Hex data:

1. In the **Hex View** tab, select the segment of data that you want to decode.
2. In the **Values** tab at the bottom of the Hex view tab, scroll to the desired encoding, then click ⊞ to expand the display.



Some encoding options have sub-decoding categories.

3. Click or to expand or collapse all the encoding types.
4. To decode a different segment of data, select another segment in the **Hex View** tab.

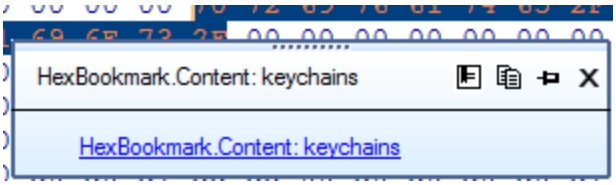
   The results in the **Values** tab change to reflect the selected segment.

12.6. Viewing the hex data information

Display the information of bookmarked segments and search results when you point to them in the **Hex View** tab.

1. In the Hex View tab toolbar, click .
2. Position the mouse over bookmarked information or search results in the Hex.

   The floating information frame appears.



   The following information includes:

   - Links (pointers) to analyzed data items such as files and folders in the project tree.
   - Search results associated with the pointed data.

3. To edit the bookmark, click .
4. To copy the data, click .

   The data is copied to the clipboard.

5. To pin the information frame open, click ⊹.

   The information frame remains open and displays the information for the last segment that you point to. The information displayed in the frame is automatically updated when you point to a different bookmarked segment or search result.

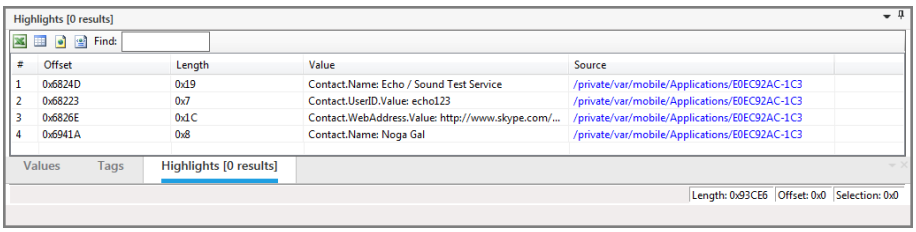
6. To close the information frame, click ✕.

12.7. Locating specific data types in the Hex

The **Highlights** tab presents analyzed data locations within the Hex data, enabling you find the exact location(s) of a particular type of analyzed data in the Hex data.

1. Access the **Highlights** tab at the bottom section of the Hex view.
2. In the project tree, select one of the **Analyzed Data** folders, for example, **Contacts.**

   The selected folder is highlighted in the **Hex View** tab; the **Highlights** tab lists the chunks in the selected folder.



3. To export the Highlights list, click the desired output in the **Search** tab toolbar: Excel, HTML, PDF, or XML.

13. Camera and screenshot evidence

Cellebrite UFED together with the UFED camera enables you to collect evidence by taking pictures or videos of a device. A screenshot feature captures internal screenshots directly from a BlackBerry, Android or iOS device. These options can be useful as complimentary evidence or in instances when data cannot be extracted from a device. This evidence can be displayed in Physical Analyzer together with any notes, categories and bookmarks, which were added by the examiner. For information on capturing camera and screenshot evidence, refer to the *Cellebrite UFED 4PC* or *Cellebrite UFED Touch* user manuals.

To import camera or screenshot evidence:

» Click the Evidence.ufd file.

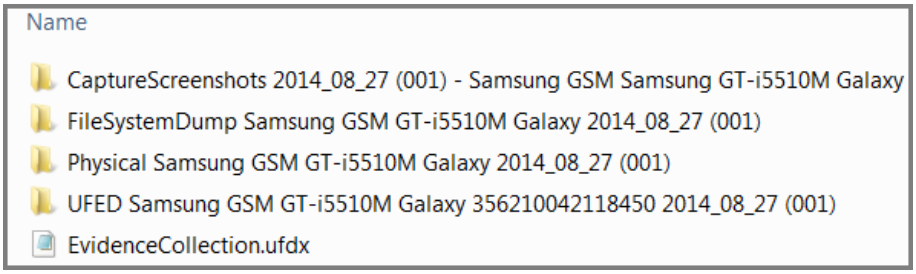
The Camera Evidence (pictures and videos) or Phone Evidence (screenshots) is imported into Physical Analyzer as a new project. The evidence includes Phone Evidence or Camera Evidence divided by category, as well as entity bookmarks and notes that were added during the extraction.

To import camera and screenshot evidence together with the extracted data:

» Click the EvidenceCollection.ufdx file.

The Camera Evidence (pictures and videos), Phone Evidence (screenshots) and the extracted data are imported into Physical Analyzer as a single project. The evidence includes Phone Evidence and Camera evidence, as well as categories, entity bookmarks and notes that were added during the extraction.

> Drag-and-drop the EvidenceCollection.ufdx file into Physical Analyzer to open multiple extractions, which were performed for a particular device. That is, all extractions in the folder will be opened. Each extraction (.ufd file) in the folder can also be opened separately. An example folder with multiple extractions and a UFDX file is displayed next.



14. Advanced decoding

This section explains the following:

Managing chains (below)

Plug-ins (on page 416)

Using the Python shell (on page 418)

Exporting the file system (on page 419)

Using the Android unlock pattern carver plug-in (on page 419)

Android unlock password carver plug-in (on page 420)

These feature are available with Physical Analyzer only.

14.1. Managing chains

A chain is a set of plug-ins grouped together, which is used to process the extracted data of a device. Each device in the supported devices list of the application has a predefined parsing chain assigned to it.

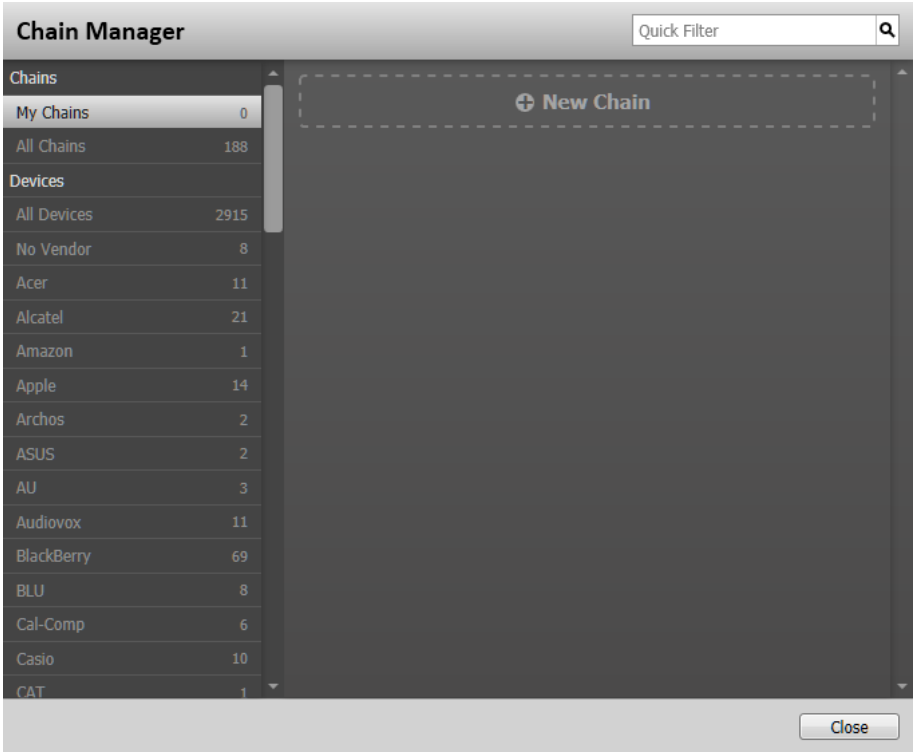
As part of its building blocks, a chain can also include other predefined chains.

Use the Chain manager to:

- Manage and edit existing chains
- Create new chains
- Assign chains to devices

To manage application chains:

1. Do one of the following:
   - In the **Plug-ins** menu, select **Chain manager**.
   - Click . The Chain manager window appears.



The **Chains** list on the left enables you to filter the displayed chains list.

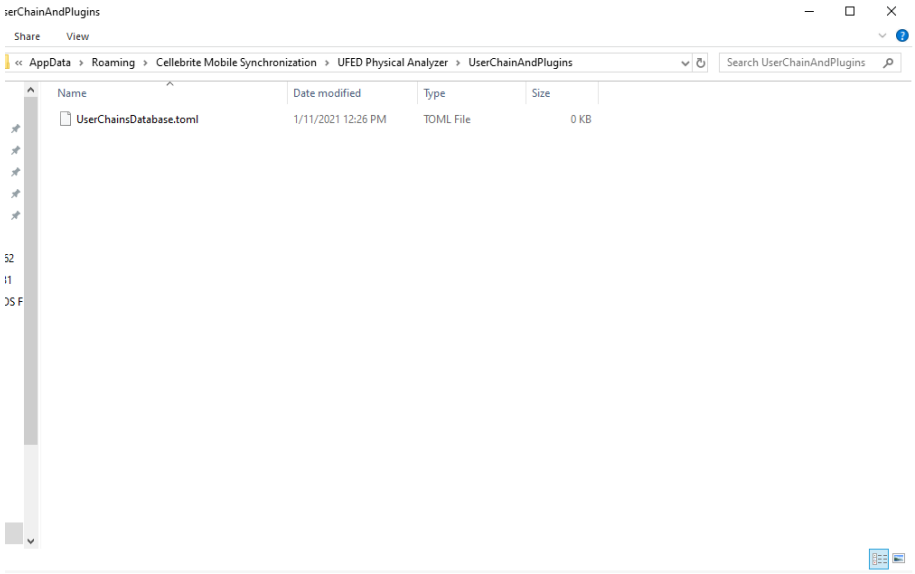
2. Click **My Chains** to display your custom chains.
3. Click **All Chains** to display a list of all the predefined chains.
4. Use the **Quick Filter** box at the top left of the window to filter the displayed list of chains.
5. To display the chains assigned to a specific device, from the Devices section of the list, select one of the following:
   - **All Devices** to display a list of all the predefined devices.
   - A manufacturer name to display a list of the predefined devices of the selected manufacturer.
6. Double-click on a device to display its chains window.

   The chains window of the device displays at least one chain that was assigned to it.

Chains management is separated to two sections:

- Cellebrite default chains
- User customized chains

The User customized chains are saved as a TOML file in the user's "App Data" folder and will not be overwritten when upgrading Physical Analyzer version.



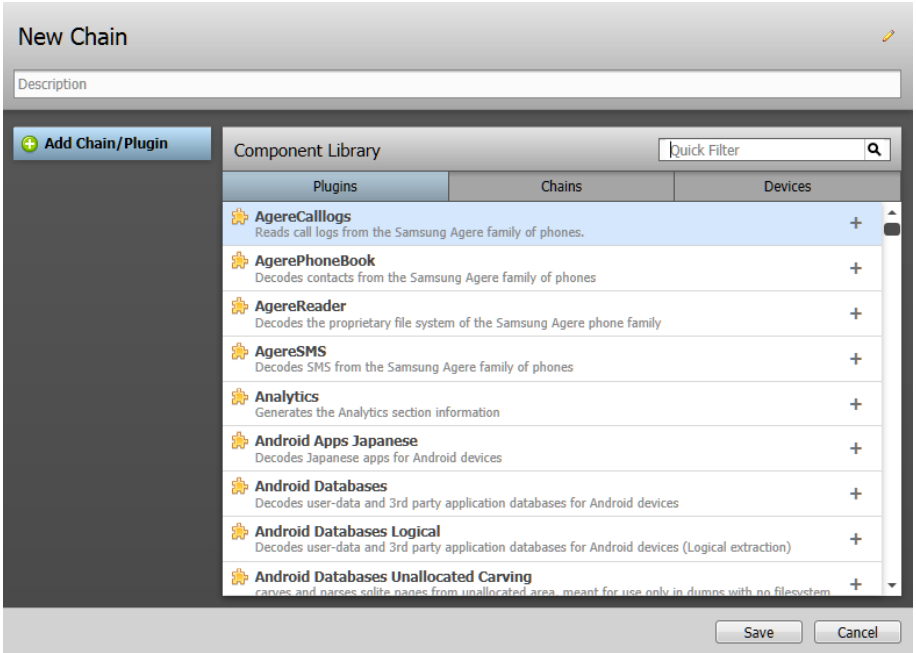
When editing or creating a chain, the TOML file will be updated once the Physical Analyzer instance will be closed. It is therefore recommended to have only one Physical Analyzer instance open when updating/customizing user chains. Close the Physical Analyzer instance once chain customization is complete to apply the changes.

> Having multiple Physical Analyzer instances open can create a situation with different state of updates to the user chains file. This can override the user's intended update.

> If user's TOML file will be corrupted (manually edited incorrectly or corrupted by an external process) Physical Analyzer will override the user's chain file when loading to a clean state.

14.1.1. Constructing a new chain

1. In the Chain manager window, click **New Chain**.
2. Click **New Chain**. The New Chain window appears.



3. Click **New Chain** at the top of the window, and enter a name for the chain.
4. In the **Description** box, enter a short description for the chain (optional).
5. From the Component Library, select a components category:
   - **Plugins** - Specific plug-ins.
   - **Chains** - Specific predefined chains.
   - **Devices** - Entire chain of specific plug-ins.

> **Devices** and **Chains** are added to the chain as a chain component.

6. To add a component to your chain list, click + next to the component.
7. To remove a component from the chain list, click × at the right of the component item, then click **Yes** to approve.
8. To edit the parameters of a plug-in or chain, select it from the chain components list (on the left) and set the options displayed.

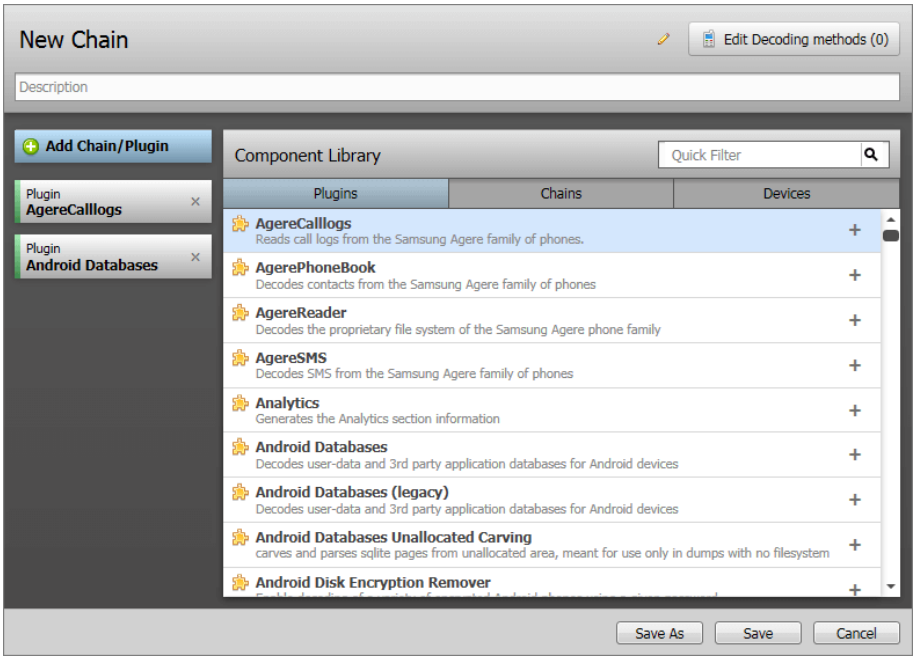
> To return to the Component Library display and continue adding more plug-ins and chains, click **Add Chain/Plugin**.

9. When finished, click **Save**. The new chain is added to your My Chains list.

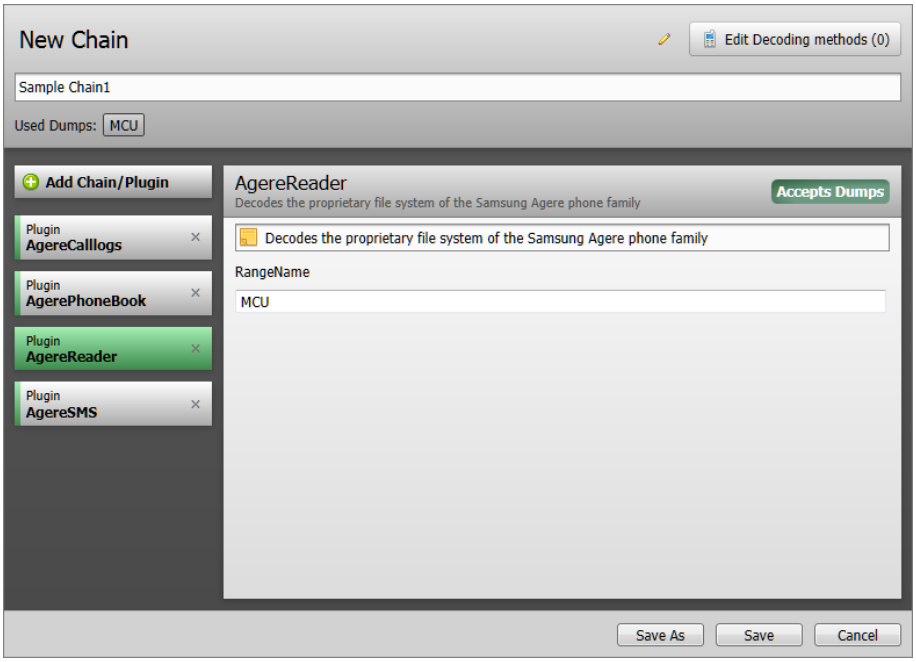
14.1.2. Editing an existing chain

To edit chains that you have created:

2. In the Chain manager **My Chains** list, double-click the chain you wish to edit.
3. Click **Add Chain/Plugin** to display the Component Library.



4. To add a component to your chain list, click + next to the component.
5. To remove a component from the chain list, click × at the right of the component item, then click **Yes** to approve.
6. To edit the parameters of a plug-in or chain, select it from the chain components list (on the left) and set the options displayed.



To return to the Component Library display and continue adding more plug-ins and chains, click **Add Chain/Plugin**.

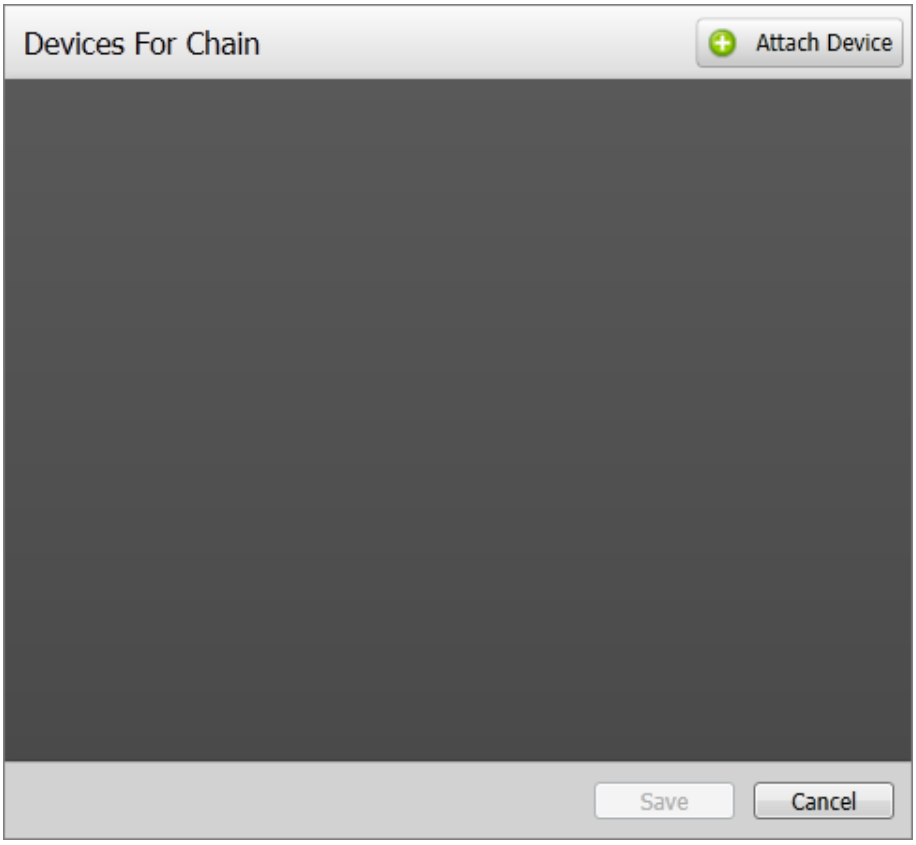
7. When finished, click **Save**, or **Save As** to save the edited chain as a new chain.
8. If you selected **Save As**, enter a name for the new chain and click **Save**.

> Changes made to factory predefined locked chains can only be saved as a new chain.

14.1.3. Attaching devices to a chain

You can attach devices to chains you have created, or modify device chains and save them as a copy.

1. Double-click the chain to which you want to attach a device.
2. Click **Edit Devices**. The following window appears.

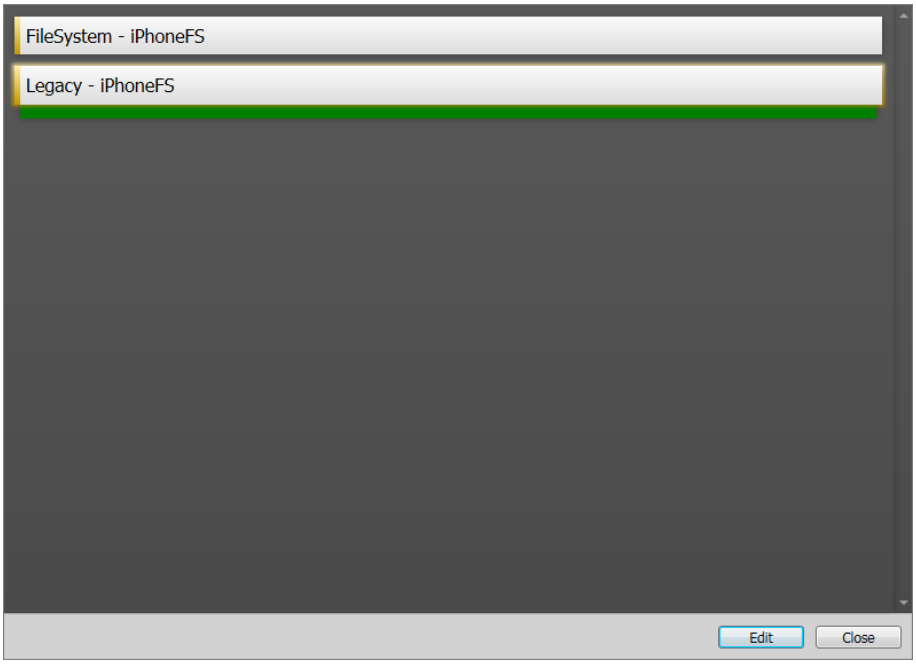


3. In the Devices For Chain window, click **Attach Device**.

4. In The Select Device window, select the device you would like to attach to the chain and click **Select**.
5. Repeat steps 3 and 4 to add more devices.
6. When you have finished attaching the devices, click **Save**.

14.1.4. Setting the default device chain

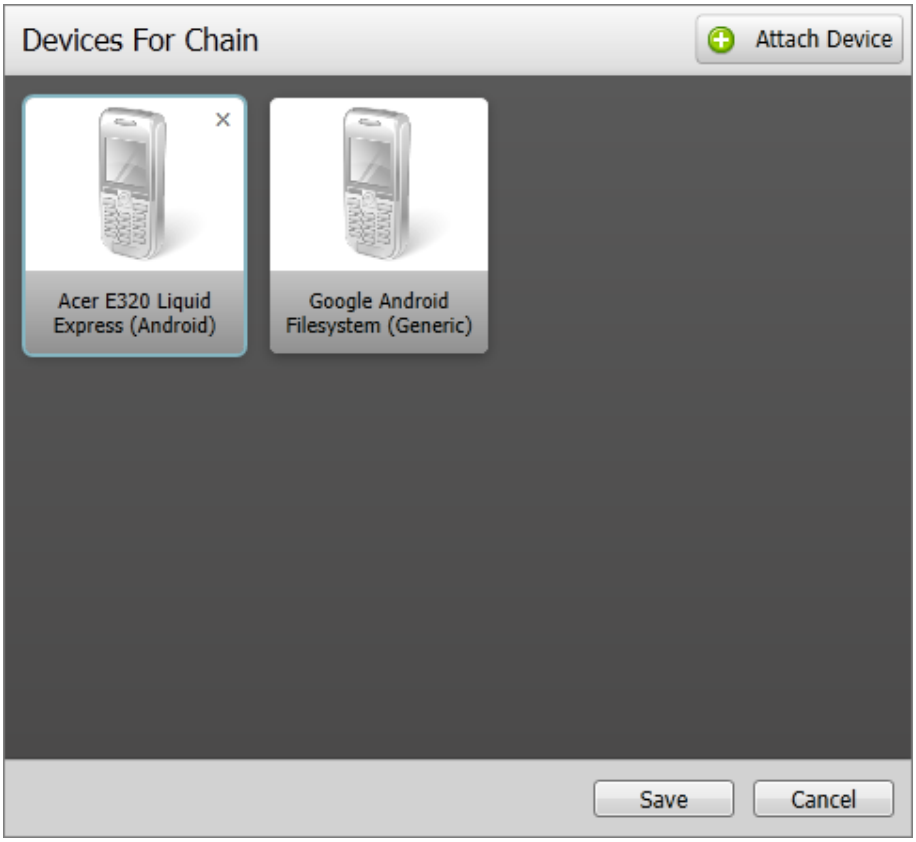
1. In the Chain manager window, use the Devices list to locate the device you wish to modify.
2. Double-click on the device to display its chains window. The following window appears.



3. If the chains list of the device contains more than one chain, click ✔ to set it as the default chain of the device.
4. Click **Close** to close the device chains window.

14.1.5. Detaching devices from a chain

1. Double-click on the chain from which you wish to detach a device.
2. Click **Edit Devices** at the top right of the chain window. The following window appears.



3. Click × at the right of every device you wish to detach from the chain.
4. Click **Close**.
5. Click **Cancel** to close the chain window.

14.1.6. Removing a chain

You can remove chains from the My Chains list only.

1. In the Chain manager window, select **My Chains**.
2. Click × at the right of the chain.

14.1.7. Chain descriptions

The following table lists selected UFED device chains and descriptions.

Chain name	Description
Android Generic	Decodes generic chains for Android devices.
Android Logical with Content	Decodes content for Android logical extractions.
Android Samsung Nexus	Decodes Samsung Nexus devices.
AndroidADB Backup	Decodes the Android ADB backup file.
AndroidContent	Decodes content for Android file systems.
AndroidDD	Decodes certain types of Android devices using the metadata from the extraction.
AndroidFS	Decodes different file systems on Android. This is part of Motorola Android or AndroidDD chains.
AndroidFSR	Decodes Android devices with the FSR flash translation layer.
AndroidFSR JTAG	Decodes JTAG extractions of Android phones with the FSR flash translation layer.
AndroidiDen	Decodes Motorola iDen with Android operating system physical extractions.
AndroidMotorolaYaffs	Decodes Motorola Android device (AndroidDD) extractions.
AndroidMTK MMC	Decodes MMC extractions of MTK Android devices.
AndroidMTK NAND	Decodes NAND extractions of MTK Android devices.
AndroidNvidia	Decodes Android devices with an Nvidia chipset.
AndroidSamsungFAT	Decodes various Samsung Android phones with FAT file systems.
AndroidXSR	Decodes Android devices with the XSR flash translation layer.
AndroidXSR JTAG	Decodes JTAG extractions of Android phones with the XSR FTL.
BlackBerry Filesystem Content	Decodes data from BlackBerry file systems.
BlackBerry Physical	Decoding BlackBerry physical and/or file system extractions.
BlackBerry10 Backup	Decodes BlackBerry10 bbb Backup files.
BlackBerry10 Content	Decodes content from BlackBerry10 devices.

Chain name	Description
BlackBerry10 Physical	Decodes the partitions and file system.
BlackBerryBackup	Decodes BlackBerry backup extractions.
BlackBerryIPD	Decodes BlackBerry backup devices using Cellebrite's default chain.
CasioC700Content	Decodes models for the Casio c7X1 series.
Garmin	Decodes GPS data from Garmin devices.
Generic FAT	Decodes FAT (file allocation table) system.
HTC Generic JTAG	Decodes the extraction in all supported methods for HTC devices.
iCloudBackup	Decodes data from Apple iCloud backup.
Infineon V2	Decodes data from Infineon devices.
iPhone Content	Decodes content for iPhones.
iPhone Databases Logical	Decodes iPhone content for logical extractions.
iPhone Logical Backup	Decodes iPhone logical report extractions with databases.
iPhone Logical with Content	Decodes iPhone logical report extractions.
iPhoneBackup	Decodes data from iPhone backup.
iPhoneBackupLogical	Decodes data from iPhone backups for logical extractions.
iPhoneFS	Decodes iPhone file systems and content.
iPhonePhysical	Decodes Physical iPhone extractions.
Kyocera S2300 Content	Decodes Kyocera S2300 SMS.
LG Qualcomm JTAG with Content	Decodes file system and content from JTAG extractions of LG Qualcomm devices.
Mass Storage Device Filesystems	Decodes standard file systems from physical mass storage device extractions.
Mio	Decodes data from Mio devices.
Motorola Android	Decodes Motorola Android devices.
MTK Generic	Decodes data from MTK devices.
Navitel	Decodes data from Navitel GPS devices.

Chain name	Description
Nokia Content	Decodes all Nokia content.
Nokia FS	Decodes Nokia file systems.
Nokia Physical with Content	Decodes physical extractions of Nokia devices.
Nokia Predef Content	Decodes content of Nokia Predef devices.
Nokia Predef XSR	Decodes non Symbian Nokia BB5 physical extractions.
PantechCdm8999Contents	Decodes SMS, MMS and call logs for the Pantech CDM8999 device.
QCAndroid	Decodes Qualcomm Android physical extractions.
QCAndroid JTAG	Decodes JTAG extractions of Qualcomm Android devices.
Qualcomm EFS ZTE with SMS	Decodes raw EFS and ZTE SMS.
Qualcomm Physical JTAG	Decodes JTAG extraction of Qualcomm devices.
Qualcomm Winmobile	Decodes the flash translation layer of LG Windows mobile and extracts files and SMS from the file system.
Report	Decodes reports into Physical Analyzer.
Report with ADB Backup	Decodes logical extractions and ADB Backup on Android devices.
Samsung Generic JTAG	Decodes the extraction in all supported methods for Samsung devices.
Samsung MCUv2 - No MMS, Phonebook	Decodes MCUv2 devices excluding MMS and phonebook.
Samsung MCUv3 Content	Decodes content from MCUv3 file system.
Samsung MCUv3 Physical	Decodes the file system from MCUv3 extractions.
Samsung MCUv3	Decodes a file system from MCUv3 extractions.
Samsung Non Android Content	Decodes content of Samsung devices that are not running Android operating systems.
Samsung Qualcomm JTAG with Content	Decodes file system and content from JTAG extractions of Samsung Qualcomm devices.
Samsung Qualcomm with Content	Decodes file system and content from Samsung Qualcomm devices.

Chain name	Description
Samsung Qualcomm with SMS	Decodes file system and SMS from Samsung Qualcomm devices.
Sanyo Qualcomm CDMA Physical	Decodes the flash translation layer file systems and content of Sanyo CDMA devices with a Qualcomm chip.
Sanyo Qualcomm JTAG with Content	Decodes content from JTAG extractions of Sanyo CDMA devices with a Qualcomm chip.
SIM Card FS	Decodes content from file system extractions of SIM cards.
Symbian databases	Decodes content databases for Nokia Symbian devices.
Symbian Physical	Decodes the flash translation layer and a FAT partition using Symbian.
Symbian XSR JTAG	Decodes JTAG extractions of Symbian phones with the XSR flash translation layer.
UMX content	Decodes content from UMX devices.
WebOS	Decodes file systems for Web operating system devices (Palm).
Windows Mobile XSR JTAG	Decodes JTAG extractions of Windows mobile devices with the XSR flash translation layer.
Windows Phone 8	Decodes extractions of Windows Phone 8 devices.
WindowsPhone7	Decodes extractions of Windows Phone 7 devices.
WindowsPhone8 JTAG	Decodes JTAG extractions of Windows Phone 8 devices.
ZTE SMS	Decodes SMS from of ZTE feature devices.

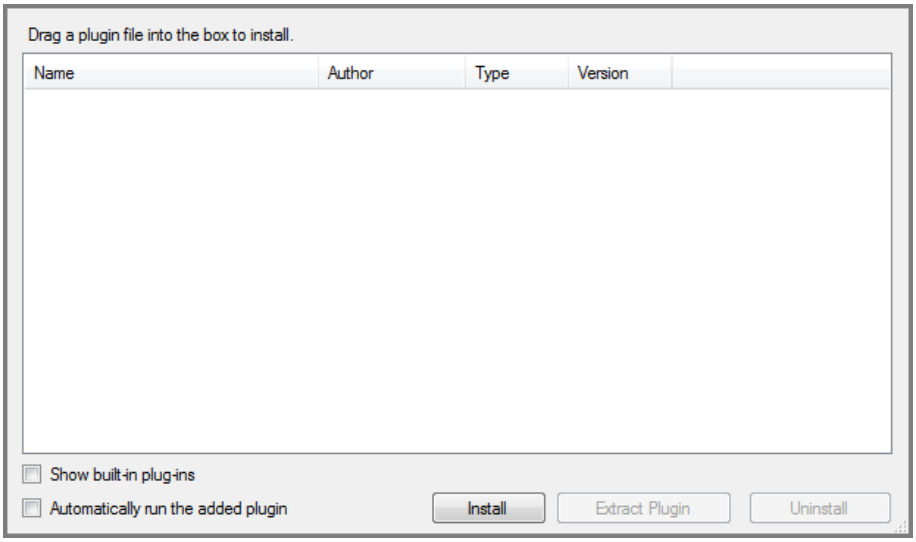
14.2. Plug-ins

The Plug-ins mechanism is an API that allows users to expand the abilities of the application by adding plug-ins provided by Cellebrite, or custom tailored plug-ins written using Python.

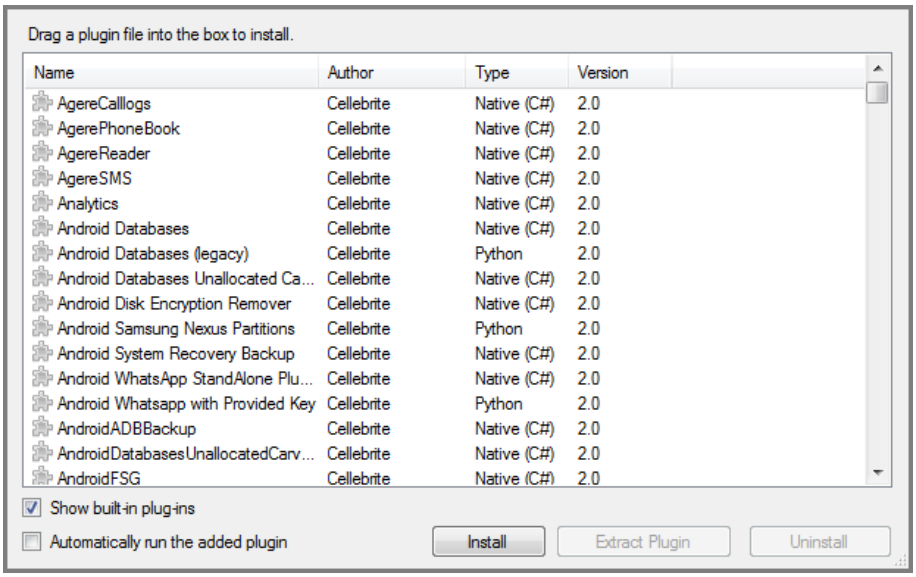
14.2.1. Managing plug-ins

The Add/Remove Plugins window enables you to manage the installed plug-ins.

1. Click . The following window appears.



2. To display all the installed plug-ins, including the built-in plug-ins that cannot be removed, select **Show built-in plug-ins**.



Perform the following tasks in the Add/Remove Plugins window:

3. To install additional plug-ins, drag them to the Add/Remove Plugins window.
4. To extract a copy of an installed plug-in, select the plug-in and click **Extract Plugin**.
5. To remove an installed plug-in, select the plug-in and click **Uninstall**.

> You cannot extract or uninstall a built-in plug-in of the application.

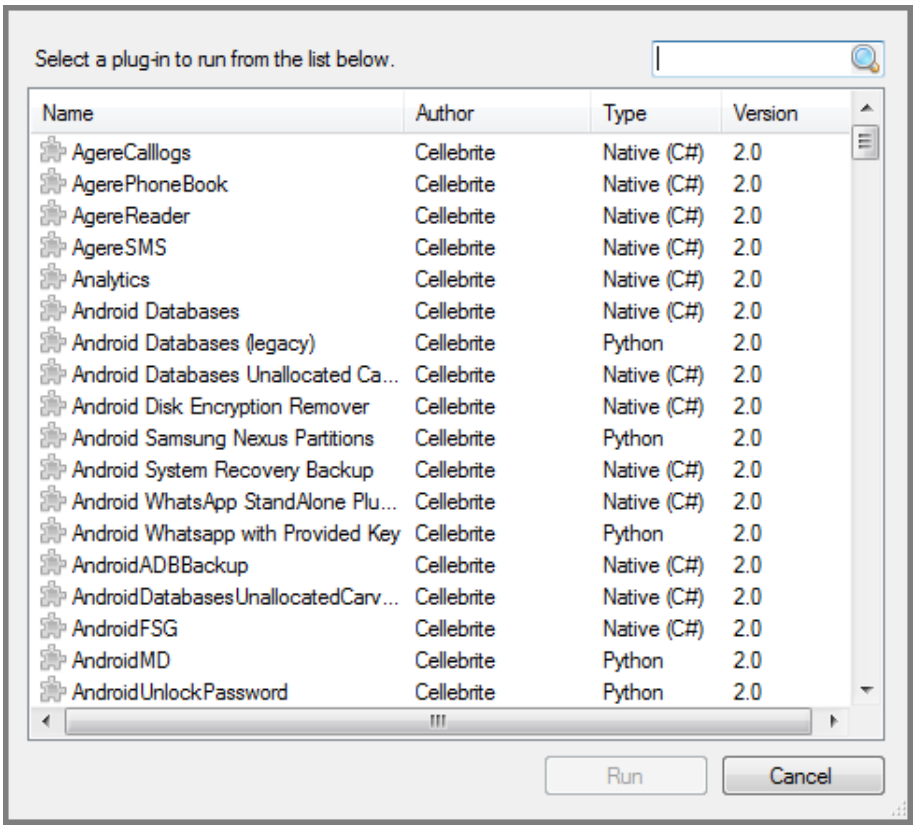
6. To display the plug-in status, double-click the plug-in.

   The Plug-in Status dialog displays the status of the plug-in, which can be either signed or unsigned.

   A signed plug-in is a plug-in that was approved and signed by Cellebrite.

14.2.2. Running a specific plug-in

1. Run an individual plug-in on your project.
2. In the **Plug-ins** menu, select **Run plug-in**. The following window appears.



3. Select the desired plug-in from the list of plug-ins, and click **Run**.

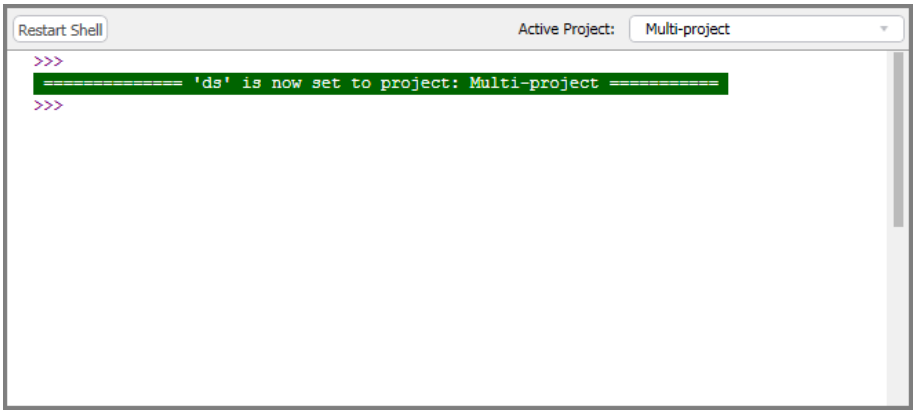
14.3. Using the Python shell

The built-in Python shell enables you to run customized decoding and analysis using Python commands.

To open the Python shell window, do one of the following:

» In the **Python** menu, select **Python shell**.

» Click . The following window appears.



For additional information on how to use Python shell commands for custom analysis, refer to the "Python Scripting Guide", accessible from the **Help** menu.

14.4. Exporting the file system

Export the extracted file system to save the entire file system to the selected location on your computer. The save provides the physical files and folders structure saved in the same hierarchy as the original file system.

To export the extracted file system:

1. In the **Tools** menu, select **Dump file system**, or click .
2. In the Browse For Folder dialog, select the target location to which to save the extracted file system.
3. Click **Make New Folder** to create a new folder in the target location.
4. Click **OK** to export the file system.

14.5. Using the Android unlock pattern carver plug-in

Use the Android Unlock Pattern Carver plug-in when working with Android devices where decoding is not yet supported.

The Android Unlock Pattern Carver plug-in can decode unlock patterns on Android devices. The plug-in can be executed on the image file created by the UFED device, JTAG, chip-off, or other tools for which decoding is not yet supported. The image file can be all device partitions, or the user data partition only.

1. Perform physical extraction using the UFED unit.
2. In Physical Analyzer, open the Android physical extraction either by dragging and dropping, or by using the "Open Advanced" option.
3. Run the **Android Unlock Pattern Carver** plug-in. For more information on running a plug-in, see Running a specific plug-in (on the previous page).

   The unlock pattern is presented in the **Extraction Summary** tab **Device Info** area.

4. Unlock the Android device, and perform a physical or file system extraction using the UFED device.

14.6. Android unlock password carver plug-in

Physical Analyzer includes the Android Unlock Password Carver plug-in. The plug-in, developed by the CCL Forensics group and integrated into Physical Analyzer by Cellebrite, attempts to extract the unlock passwords from Android extractions. The plug-in can be found in the standard plug-ins list.

15. Settings

The Settings window provides a set of functional and behavioral setup options used to fine-tune and control the functionality and usability of the application. The settings in the Settings window apply to all the projects open in Physical Analyzer.

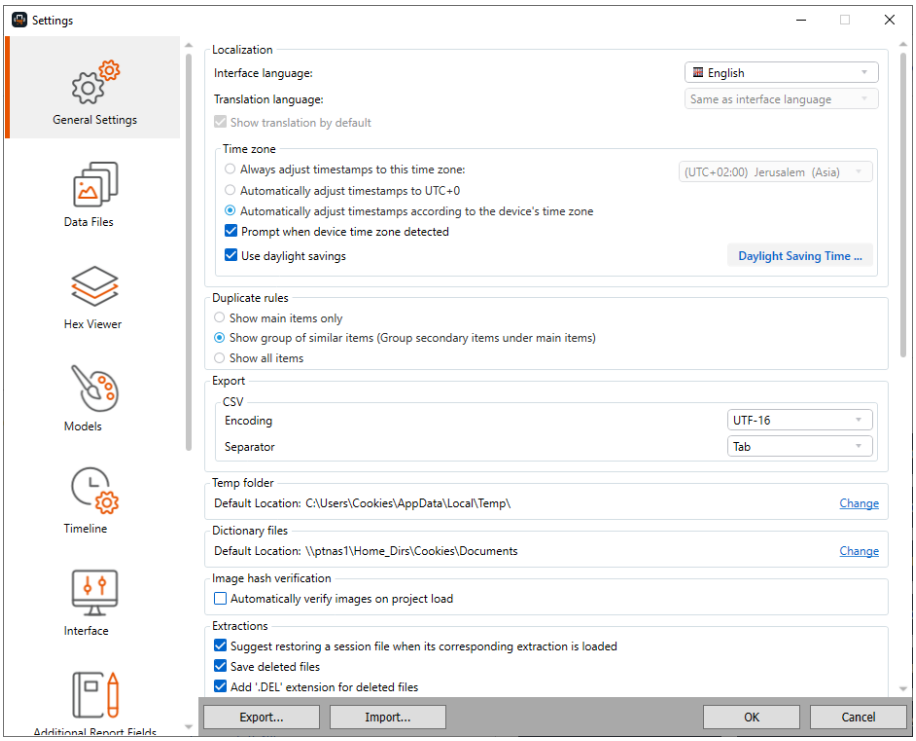
> Changes to settings are lost when you close Physical Analyzer. To save the settings configuration, see Saving settings (on page 445).

To access the Settings window:

» Select **Tools** > **Settings.**

15.1. General settings

Set general application settings in the **General Settings** tab.



Localization

To set the interface language of Physical Analyzer:

» In the Localization area, in the **Language** list, select the desired interface language.

To set the translation language:

1. In the Localization area, select the Translation language. That is the language to which you want to translate the text. You can only select one Translation language. To request additional translation languages, select **Get more languages**.
2. Select the **Show translation language by default** check box to display translations by default. Clear this check box so that the translation will not appear when you translate text. To see the translation select **View translated**.

> The **Smart Translator automatic language detection** check box is selected by default and automatically identifies the Smart Translator language to which you want to translate. To manually select the Smart Translator language, clear the check box.

Time zone

To shift timestamps and enable daylight saving time:

1. In the Time zone area, from the Time zone settings (UTC) list, select one of the time zones (UTC -11:00 to UTC +14:00) to recalculate network-defined timestamps according to the time zone offset.
2. Select the **Automatically adjust timestamps to UTC+0** check box, to automatically adjust timestamps to UTC+0. This setting is recommended when working on multiple extractions so that all records will be presented according to the same adjusted time zone offset.

> This check box is selected by default, but is disabled if the Always adjust timestamps to this time zone check box is selected.

3. To automatically adjust timestamps to the device's time zone, select the **Automatically adjust timestamps according to the device's time zone** check box. When this check box is selected, all timestamps will be adjusted to the mobile device time zone, including report outputs.

> If the time zone of the device is identified during decoding, then a message is displayed allowing you to adjust all extractions to the devices time zone.

4. To enable the daylight saving time, select the **Use daylight savings** check box.
5. To change the start and end dates for daylight saving time, click **Daylight Saving Time**. For more information on how to change the time zone settings, see Setting a unified time zone for the project (on page 445).

To use the device's time zone if detected:

» In the Time zone area, make sure that the **Prompt when device time zone detected** check box is selected.

Multiple extractions

To change the multiple extraction settings:

1. In the Multiple extractions area, select the **Open a UFDX file** check box to open multiple extractions as a single project. If this check box is not selected all extractions will be opened as independent extractions. By default, this check box is selected.
2. In the Multiple extractions area, select the **Remove duplicates** check box to eliminate deduplications (duplicate or redundant information) in the project. Clear this check box to show the deduplications in the project. By default this check box is not selected.

To merge or group items:

» In the Multiple extractions area, make sure that the **Merge** check box is selected. This option is relevant to both decoding and reporting.

Export

To set the encoding and separator of exported CSV files:

1. In the Export area, select the desired encoding option from the **Encoding** list.
2. Select the desired separator in the **Separator** list

Temp folder

To set the temp folder location to be used:

1. In the Temp folder area, click **Change**.
2. Select the temp folder location.
3. Click **Select folder**.

> If the selected folder is deleted or inaccessible at any given time, an automatic fallback to the Windows default temp folder will be performed. You will then need to re-select the folder or a new path as necessary.

Dictionary files

To change the default location of the dictionary files:

» In the Dictionary files area, click **Change** and select a new location to be used when creating dictionaries.

Image hash verification

To automatically verify images on project load:

» In the Image hash verification area, Select the **Automatically verify images on project load** check box.

Extractions

To offer to load a session file (that was saved in the folder where the extraction is located) when opening its corresponding extraction:

» In the Extractions area, select **Suggest restoring a session file when its corresponding extraction is loaded**.

To set how deleted files are handled:

1. In the Extractions area, select the **Save deleted files** check box to save deleted files.
2. Select the **Add '.DEL' extension for deleted files** check box to save deleted files with the *.DEL extension.

Thumbnail cache

To set the number of extractions for the cached thumbnails in a project:

» In the Thumbnails area, select the number of extractions from 5 to 20. The default is 10.

If you do not want to save the cached thumbnails:

» In the Thumbnails area, clear the **Save cached thumbnails in project** check box.

If you do not want to load the thumbnail cache to memory (to conserve disk space):

» In the Thumbnails area, clear the **Load thumbnail cache to memory** check box.

Highlight information

To disable information highlighting:

» In the Highlight information area, select the **Disable highlight information** check box.

To can change the default location for the highlights database files:

» In the Highlights information area, click **Change** and select a new location to store the dedicated highlights databases (for memory ranges and highlights Information). This requires additional temporary disk storage (that will be automatically deleted once you close the application).

Views

Selected entities are included in reports or results.

To select all entities by default to be including in reports, for all views:

» In the Views area, select the **Check all entities by default** check box.

To remove cloud data sources from results:

» In the Views area, clear the **Display cloud data source results** check box.

To disable the What's new page:

» In the Views area, select the **Disable What's new** check box.

Data enrichment

Enable or disable the conversion of BSSID values and cell towers to physical locations.

To convert BSSID and cell tower values to physical locations:

» Select the **Convert BSSID values (wireless network) to physical locations** check box.

To set the BSSID window to appear:

» Select the **Show the Convert BSSID (wireless networks) and cell tower values window** check box. The window will appear upon startup.

» Select the **Show the Export BSSID (wireless networks) and cell tower values window** check box. The window will appear upon opening a relevant extraction.

Map

To display maps for extractions with location data:

» In the Map area, select the **Use maps** check box.

To use the offline maps option:

» In the Map area, select the **Use offline maps** check box.

Decoding

To recover deleted data from Android devices via carving:

» In the Decoding area, select the **Recover deleted data for Android devices via carving from unallocated space** check box.

To remove items that were detected as false positives during carving:

» In the Decoding area, select the **Automatically remove items that are detected as false positive** check box.

To enable the deep carving to recover deleted records from SQLite files:

» In the Decoding area, select the **Use deep carving for SQLite** check box.

> The SQLite file includes three types of pages: **Allocated pages** includes intact records, and some deleted data for a specific table, **Deleted pages** includes deleted or duplicate records, for a specific table, and **Lost pages** includes all types of data, including deleted records, but the original table of these records is unknown.
> SQLite deep carving recovers data from the Lost pages, and because of the amount of data this is a memory-based and a time consuming process. However, the user data is usually stored in Allocated and Deleted pages, and even if you do not use this option, you will receive most of the data.

To recover data from archive files:

» In the Decoding area, select the **Recover data from archive files** check box.

> This setting enables you to decode and process data from archive (zip) files, but requires additional decoding time.

To aggregate significant iOS locations:

» In the Decoding area, select the **Aggregate significant locations (iOS)** check box.

> When this setting is selected, Physical Analyzer can decode and display these locations. However, significant locations can be recovered only when performing full file system extractions of an iOS device using Cellebrite Advanced Services.

To enable AppGenie for all Installed Applications categories:

» In the Decoding area, select the **Enable AppGenie on all app categories** check box.

To parse FTS content from WeChat:

» In the Decoding area, select the **Parse FTS content from WeChat** check box.

> This setting controls the decoding of **fts_messages.db** which brings another source of data for WeChat app. This will give the potential to recover deleted and missing WeChat records and can bring duplications.

> To control the number of duplicates, unselect the **Parse FTS content from WeChat** check box.

Network

To disable network traffic (for example, will not check for new software versions):

» In the Network area, clear the **Disable network traffic** check box.

To enable Internet access for apps in the Virtual Analyzer:

Hash set

To move a hash set to another location:

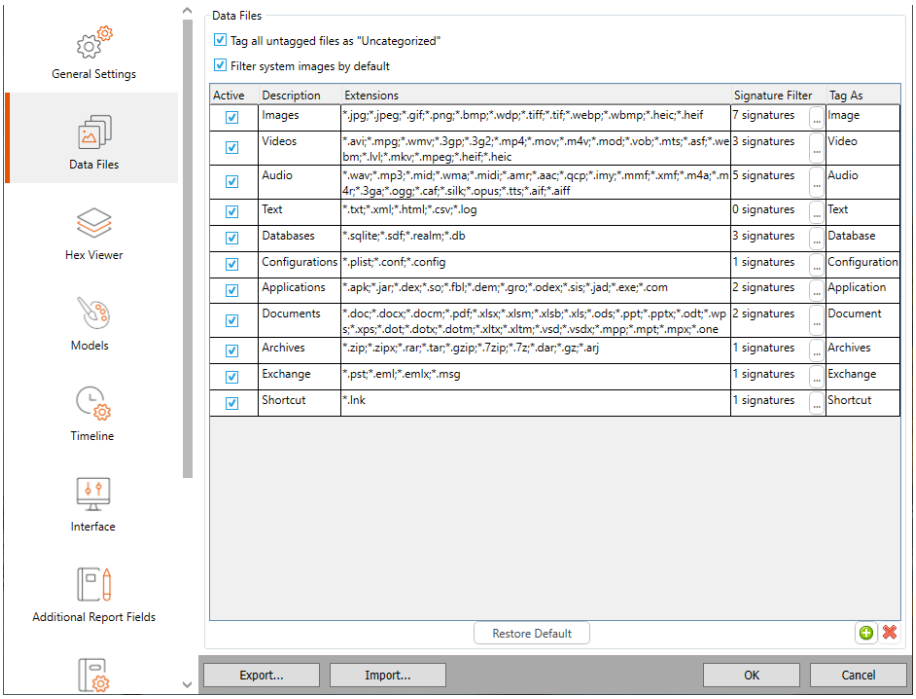
» In the Hash set area, click **Change** and select a new location for the hash set.

For more information on hash sets, see Importing and categorizing hash sets (on page 152).

To allow manual tags from a particular VIC/CAID category:

» Select the required category. The options are Project VIC US (default), UK/CAID, or Project VIC CA (Canada).

15.2. Data files



The **Data Files** settings determine the different file and tagging groups under the **Data Files** and **Tags** tree items, and the types of files filtered in each group.

Tags and filters

- Select to automatically tag untagged files as "Uncategorized."
- Select to filter system images by default.

Data file settings

Every data file record contains the following settings:

- **Active** - Indicates whether to display (checked) or hide (unchecked) this group of data files in the project tree.
- **Description** - A descriptive name for the type of data files to be used as the group name under the **Data files** tree item.
- **Extensions** - The file extensions to be used to filter the data files of this group.
- **Signature filter** - The header and/or footer signatures to be used to filter the data files of this group.
- **Tag As** - The tag name to be applied to the data file and used to list the files under **Tags** in the project tree.

15.2.1. Data files filtering methods

Groups can be filtered using one or more of the following methods:

- **Signature filter:** A signature filter is a definition of the file header and/or footer to be searched, in order to detect a file type and associate it with a specific Date File group. The header and/or footer can be configured in a defined range from the beginning and end of the file respectively by using the offset parameter.
  For example, a JPEG image starts with the header FF D8 FF and ends with the footer FF D9. Entering this information in the Header and Footer fields of the signature creates a signature that identifies JPEG images.
- **Extension filter:** An extension filter is a list of common file extensions that are associated with file formats that belong to the specific data file group.
  For example, the different image file formats can be filtered by the file extensions *.jpg, *.jpeg, *.gif, *.png or *.bmp.

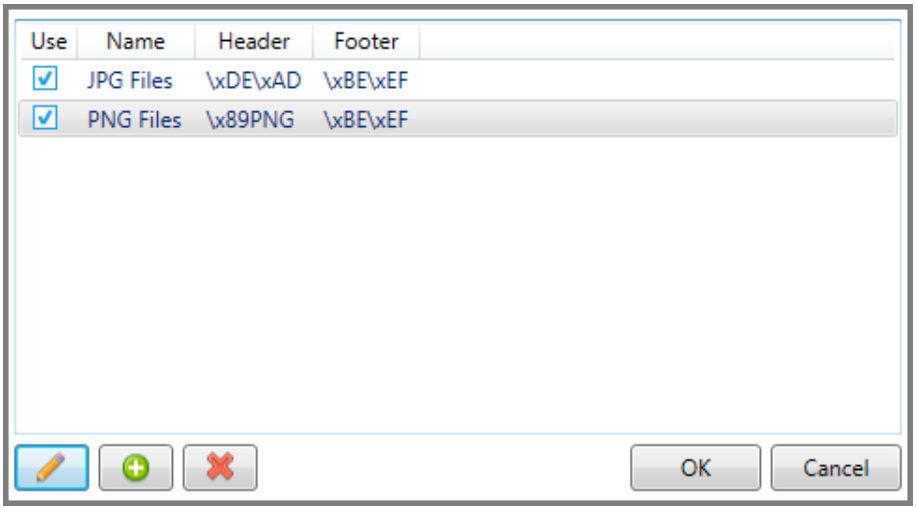
15.2.2. Managing data files settings

Add new types of data files, and edit and delete existing data file types.

15.2.2.1. Adding a new data file type

1. In the **Data Files** settings, click .

   A new row is added to the list.
2. Select **Active** to display the added data type in the **Data Type** tree item.
3. Click in the new row's **Description** box, and type a file type description.
4. If applicable, in the **Extensions** box, enter the file extensions commonly used by your data file type in the format ***.xxx**, and separated by **;**.
5. If applicable, in the **Signature filter** box, click and do any of the following:



» Click to add a filtering signature that identifies your data file type.

» Click to edit an existing signature filter.

» Click to delete a signature filter.

6. If applicable, click in the **Tag As** box, click and select a tag name from the list.
7. To change the order of the data file types, use the arrows .
8. To clear the list of data file types you added, leaving only the default types, click **Restore default**.

15.2.2.2. Editing an existing data file record

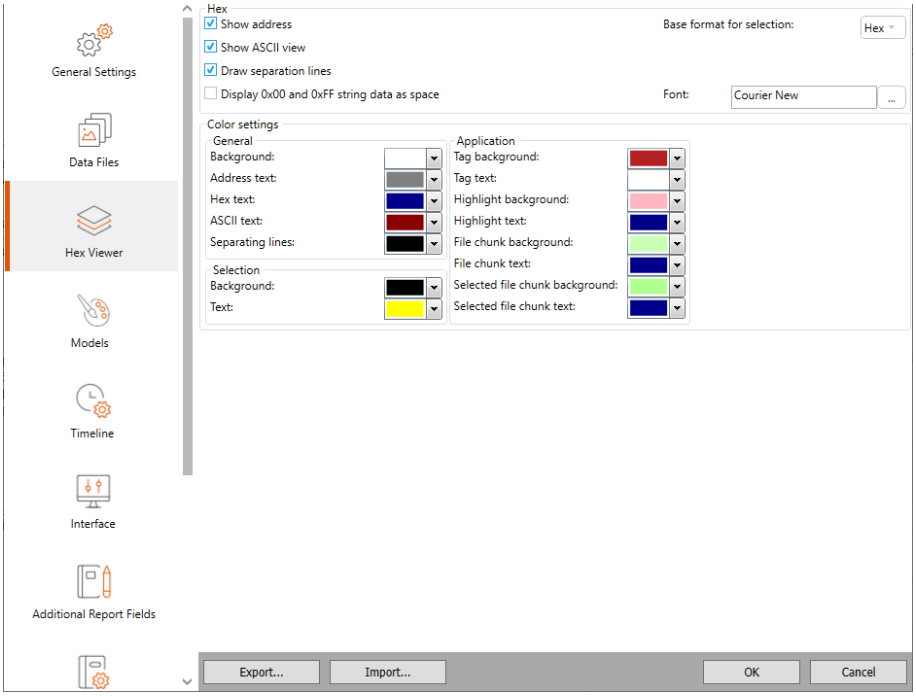
1. Click the row of the data file type that you want to edit.
2. Double-click in the column and row that you want to change, and update the existing settings as desired.

15.2.2.3. Deleting a data file type

1. Click the row of the data file type that you want to delete.
2. Click .

15.3. Hex viewer

The Hex Viewer setting enables you to control the display options of Hex extractions to suit personal preference and enhance readability.



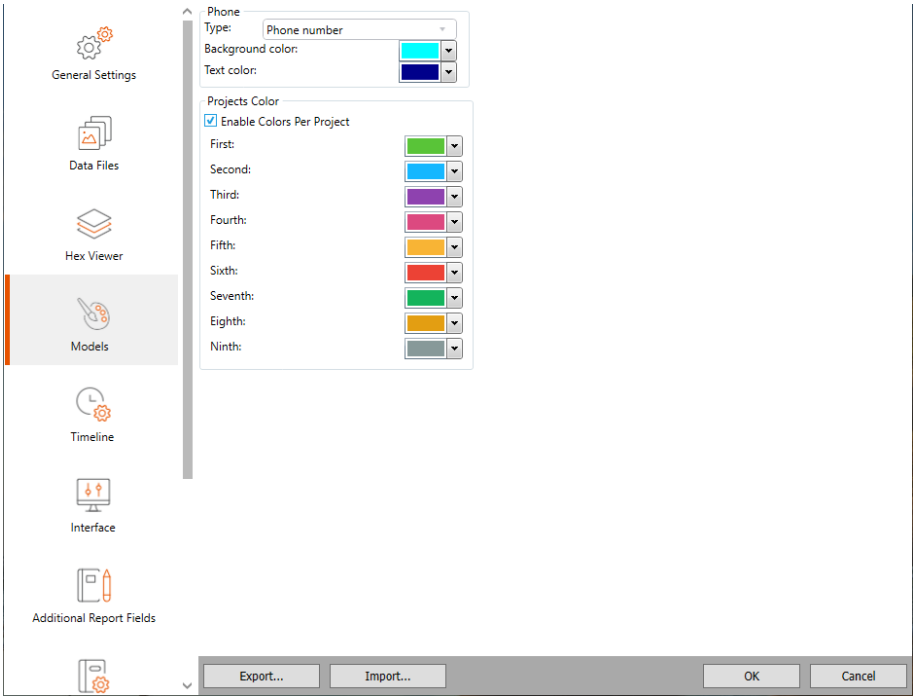
Change the defaults for the following Hex viewer settings:

- **Show address** - Show/Hide the line numbers column of the Hex Viewer.
- **Show ASCII view** - Show/Hide the ASCII view column of the Hex Viewer.
- **Draw separation lines** - Show/Hide the separation lines between the address, Hex data, and ASCII view columns
- **Display 0x00 and 0xFF string data as space** - Set the string data to display both 0x00 and 0xFF characters as space instead of a ".".
- **Base format for selection** - The line numbers format (Decimal, Hex, or Both).
- **Font** - The font used to display the information.
- **Color settings** - Set the colors applied to different features of the Hex viewer.

15.4. Models

Set the color schemes to be applied to various types of device data.

You can also manage project colors, or enable or disable the Projects color feature. With this feature, each project tab is displayed with its color and icon (excluding the Welcome page tab). The color and the icon signify to which project and information type the tab is related.



To set the color schemes to be applied to various types of device data:

1. In the **Type** list, select the data type.
2. In the **Background color** list, select the desired background color.
3. In the **Text color** list, select the desired background color.

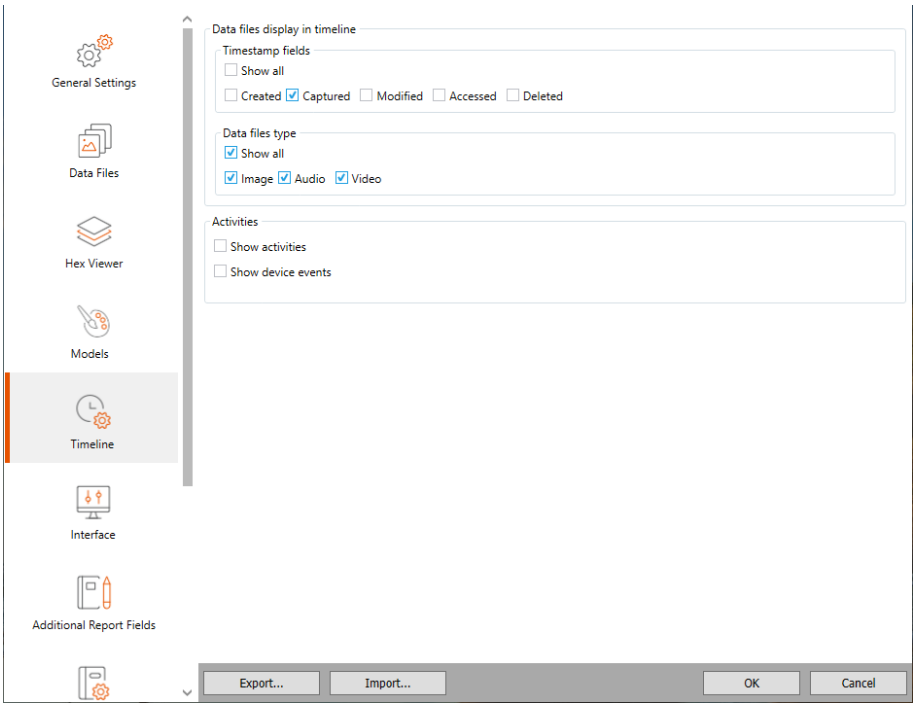
To turn off project color schemes:

» Clear the **Enable colors per project** check box.

To change a project's color scheme:

» Select the desired color for the first to the tenth project.

15.5. Timeline



The **Timeline** settings enables you to control what you see in the timeline.

Timestamp fields

Choose which timestamps to display in the timeline: All, Created, Captured, Modified, Accessed, Deleted. Only Captured is selected by default.

Data files type

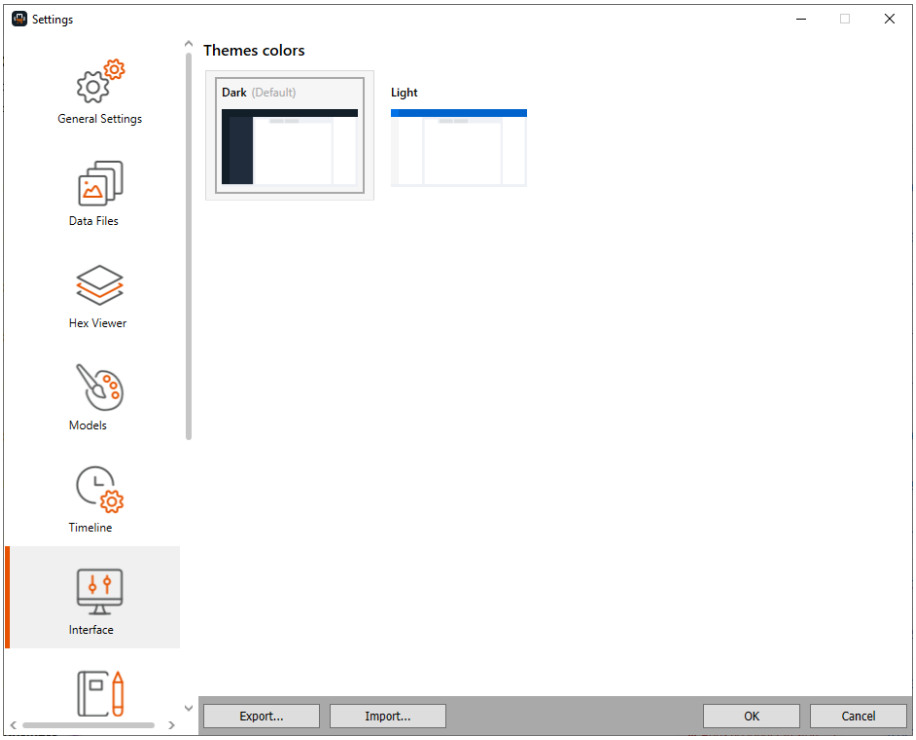
Choose which types of data files to display in the timeline: All, Image, Audio, Video. All types are selected by default.

Activities

Choose if activities are displayed in the timeline. This option is selected by default.

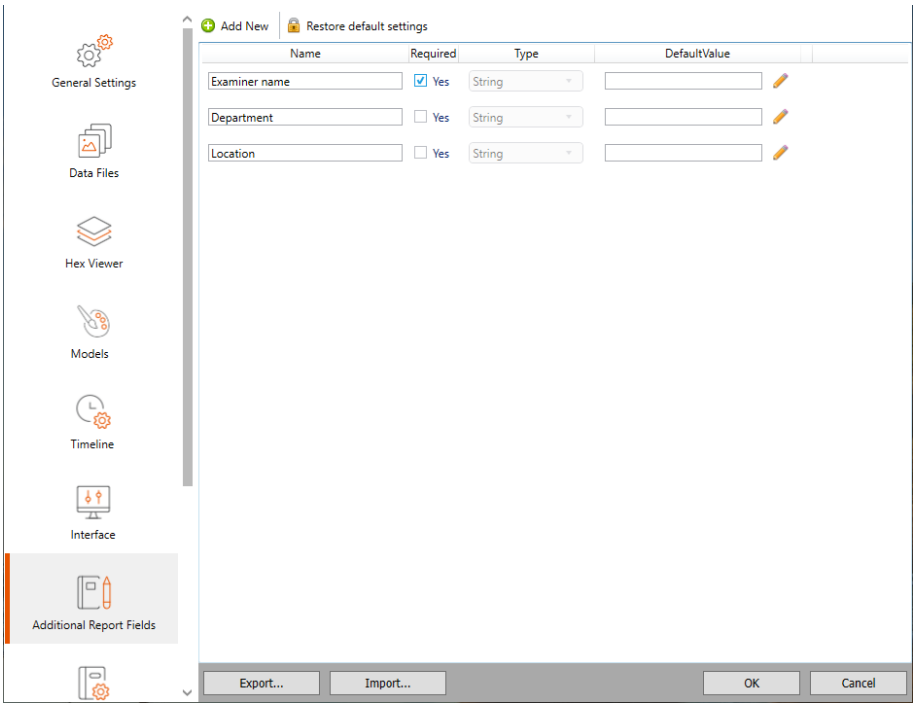
15.6. Interface

Set a theme for Physical Analyzer, either light or dark interface.



Changing the interface configuration settings, will cause the application to close and then restart.

15.7. Additional report fields



Optional information is user-defined information presented at the beginning of the report. It usually includes information about the case, investigator, and organization details.

Every optional information record consists of the following:

Name	The name of the report field.
Required	Indicates if the field must be filled in order to generate the report.
Type	The types of entry - **String** or **List**.
Default value	Default content.

You can add new report fields, and edit and delete fields, as desired.

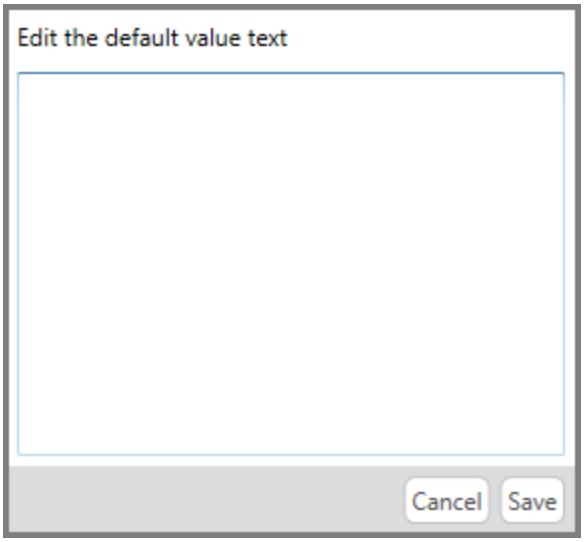
15.7.1. Adding a new report field

1. Click **Add New.**

   A new row is added to the table.

2. In the **Name** column, enter the name label to be displayed.
3. Select **Required** if this field must be filled in order for the user to generate the report.
4. In the **Type** list, select one of the following:
   - **String** for text entry fields
   - **List** for a specified list of options
5. In the **Default Value** box, set the default content:

» For **String** type, type the default string. For a multi-line string, click , enter the default string in the Option Editor, then click **Save**.



» For a **List** type, click , enter the list items with each item on a separate line, then click **Save**.

15.7.2. Editing a report field

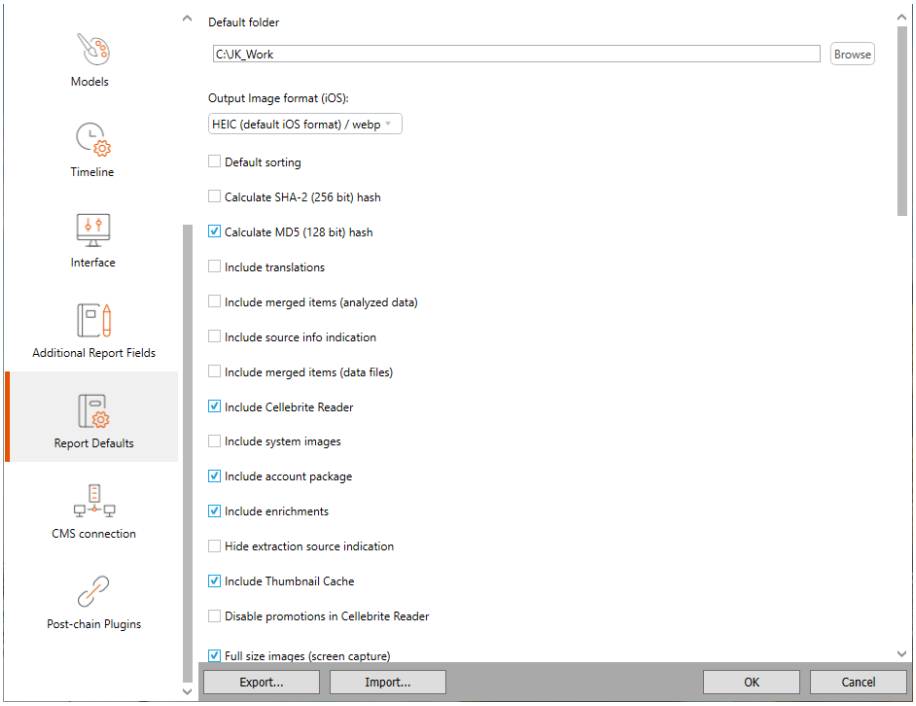
» To edit a report field, perform steps 2-5 of Adding a new report field (on the previous page), changing the parameters to suit your needs.

15.7.3. Deleting a report field

» To delete a report field, click .

15.8. Report defaults

The **Report Defaults** settings enable you to edit the report presentation.



Scroll down to see all the fields.

» In the **Report type** list, select the report type that you want to edit.

General settings

- **Default folder** - enter the path to the folder where you want to save reports you generate for this report type.
- Select **Default sorting** to set sort the items included in the generated report according to the default sorting set by Cellebrite for each of the Analyzed and Data file types or clear **Default sorting** to sort the items according to the selected sorting field and the sorting order (ascending or descending) that was set by the user in each of the data display tables.
- **Calculate SHA-2 (256 bit) hash** and **Calculate MD5 (128 bit hash)** - Select which calculated MD5 and SHA256 hash keys to add to each Data Files item in the generated report. Do not select these options to shorten the report generation process of large projects.
- **Include translations** – Select to include any translated text in the report.
- **Include merged items (analyzed data)** – Select to include merged data from the Analyzed Data area.
- **Include merged items (data files)** – Select to include merged data from the Data Files area.
- **Include Reader** – Select to share UFDR reports with authorized persons using the Reader. This option is for the UFDR format only. The Reader executable will then be included within the report output folder.
- **Include system images** – Select to include system images (images that come with the device or as part of an app installation) as well as non-system images.
- **Include account package** – Select to include an account package with user credentials, which can be used by UFED Cloud.
- **Include enrichments** – Select to include BSSID enrichment data.
- **Hide extraction source indication** – Select to hide the source file information.
- **Include Thumbnail Cache** – Select to include the thumbail cache.
- **Disable promotions in Reader** – Select to disable promotions in Cellebrite Reader.
- **Full size images (screen capture)** – Select to include full size images from the Screen capture tool.
- **Include chat bubbles** – Select to include the chat bubbles of the conversation in the report. Select **Include metadata in chat bubbles** to include the metadata.
- **Disable models categorization** - select to disable the separation and generate a report in which every data items is generated as a single section without subcategories separation. By default, a categorized report in which each category in the data items group is generated as a separate section in the report is generated. For example, when generating a report with Call logs, select the check box to generate the Call logs as a single list, or clear the check box to break it to a separate list for each category of Call logs.

For Excel reports, set the following:

- **Unprintable characters placeholder** - Set the placeholder character to replace the unprintable characters.
- **Output File Format** - Set the output file format of the spreadsheet file to either:
  * **XLSX** - The current Excel file format.
  * **XLS** - The legacy file format of Excel.
  * **ODS** - The spread file format of OpenOffice.
- **The excel report is compatible with OpenOffice** - Select to ensure the Excel report can be opened in OpenOffice.
- **Generate Contact Identification Data** - Select to add a sheet to the Excel report that provides a list of unique contacts based on type.

For HTML reports, set the following:

- **Logo Header** - Enter and format custom text to appear in the report header before the logo image.
- **Logo** - Click **Select Image File** to add the logo image to appear in the report header. Supported file formats are: BMP, JPG, GIF, and PNG.
- **Logo Footer** - Enter and format custom text to appear in the report footer after the logo image.
- **Show totals for items not in the report** - Add a **Total** column to the report that displays the total number of items that were excluded from the report.
- **Show extended deleted state** - Include the state (**Intact**, **Deleted**, or **Unknown**) of deleted items in the generated report. When not selected, logs only the state of deleted items as Yes, and is left empty for other states.
- **Number of lines for email preview** - Set the maximum number of lines from each email message to appear in the report.
- **Display full email body** - Display the entire message body.
- **Number of messages per chat** - Set the maximum number of lines per chat message to appear in the report.
- **Display all chat messages** - Display all chat messages in the report.
- **Split HTML report** - Set each section of the report to start on a new page.

For PDF reports, set the following:

- **Logo Header** - Enter and format custom text to appear in the report header before the logo image.
- **Logo** - Click **Select Image File** to add the logo image to appear in the report header. Supported file formats are: BMP, JPG, GIF, and PNG.
- **Logo Footer** - Enter and format custom text to appear in the report footer after the logo image.
- **Show totals for items not in the report** - Add a **Total** column to the report that displays the total number of items that were excluded from the report.
- **Show extended deleted state** - Include the state (**Intact**, **Deleted**, or **Unknown**) of deleted items in the generated report. When not selected, logs only the state of deleted items as Yes, and is left empty for other states.
- **Number of lines for email preview** - Set the maximum number of lines from each email message to appear in the report.
- **Display full email body** - Display the entire message body.
- **Number of messages per chat** - Set the maximum number of lines per chat message to appear in the report.
- **Display all chat messages** - Display all chat messages in the report.

For Word reports, set the following:

- **Logo Header** - Enter and format custom text to appear in the report header before the logo image.
- **Logo** - Click **Select Image File** to add the logo image to appear in the report header. Supported file formats are: BMP, JPG, GIF, and PNG.
- **Logo Footer** - Enter and format custom text to appear in the report footer after the logo image.
- **Show totals for items not in the report** - Add a **Total** column to the report that displays the total number of items that were excluded from the report.
- **Show extended deleted state** - Include the state (**Intact**, **Deleted**, or **Unknown**) of deleted items in the generated report. When not selected, logs only the state of deleted items as Yes, and is left empty for other states.
- **Number of lines for email preview** - Set the maximum number of lines from each email message to appear in the report. The report includes links to text files containing the entire email.
- **Display full email body** - Set to display the entire message body.
- **Number of messages per chat** - Set the maximum number of lines per chat message to appear in the report.
- **Display all chat messages** - Display all chat messages in the report.

15.9. Cellebrite Commander

Agencies that have several Physical Analyzer units, dispersed across single or multiple locations, can now easily and conveniently oversee and manage the distribution of software licenses and updates using Cellebrite Commander.

Cellebrite Commander is an ideal solution for organizations that want to govern internal processes and centralize the management of software updates across all deployed systems, leveraging usage and manpower. The Cellebrite Commander can be used to gather insights and usage data to help optimize planning.

Physical Analyzer together with Cellebrite Commander provides agencies with:

- One-click connectivity between Cellebrite Commander←→ Physical Analyzer
- 24/7 remote assistance by Cellebrite Commander Admin
- Software Upgrade management capabilities
- Central license management
- Reporting on iOS extractions
- Live status of Physical Analyzer units (Connected/not, updated/not)

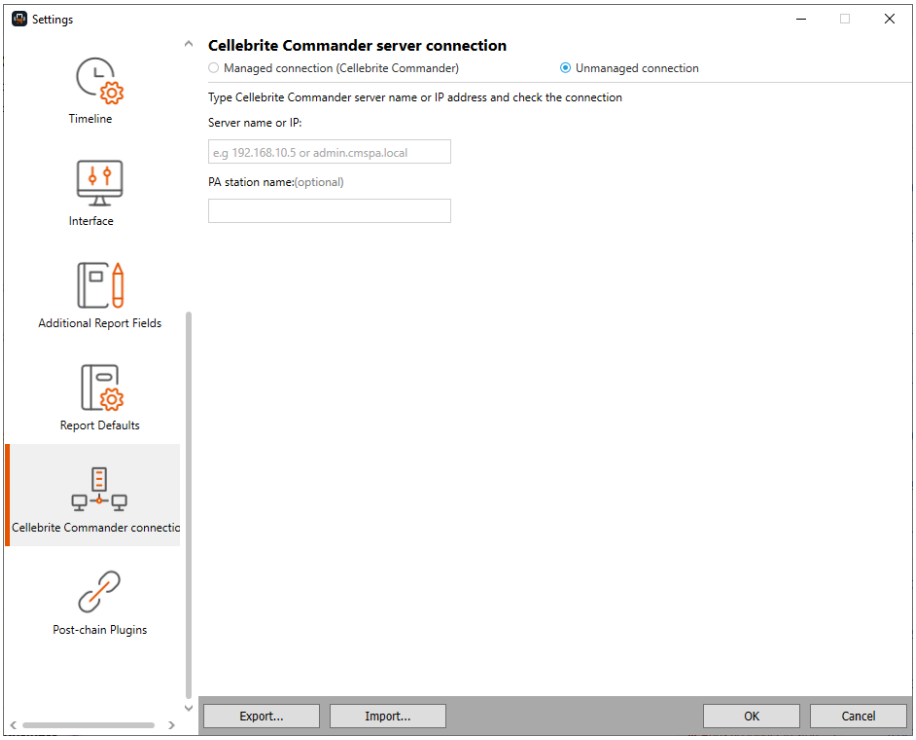
To connect a Physical Analyzer to Cellebrite Commander:

1. Go to **Tools** > **Settings** > **Cellebrite Commander connection**.

   Or

   Help > **Show license details** > **Cellebrite Commander** (tab).

   The following window appears.



2. Select **Managed connection**.

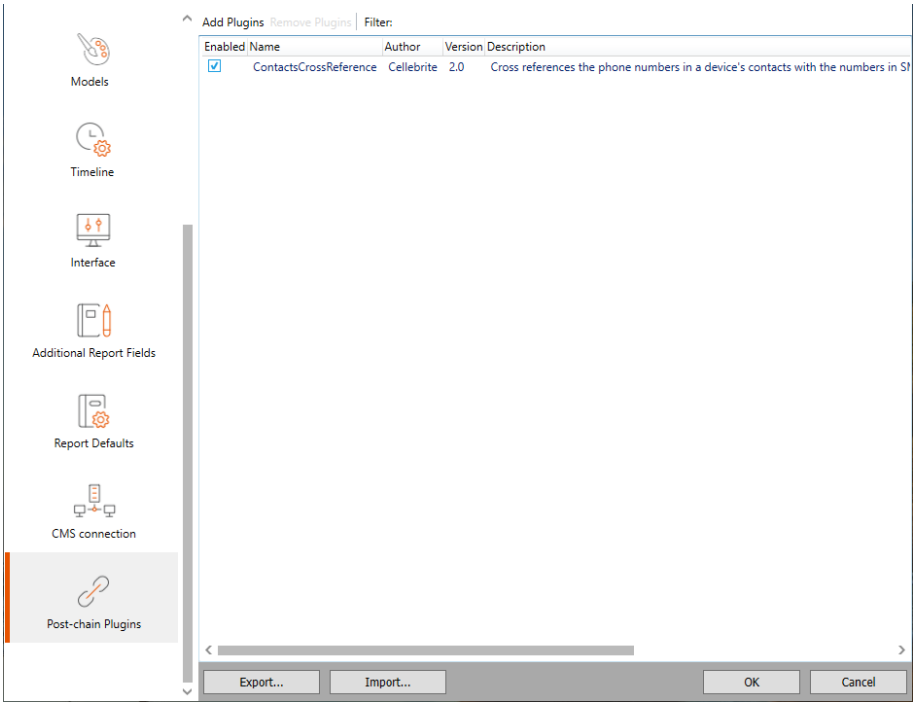
> When set to the managed connection, Physical Analyzer will be managed by Cellebrite Commander, including centralized version management.

3. Enter the Fully Qualified Domain Name (FQDN).
4. Click **Check connection**. If the validation is successful, the status changes to **Connected to Cellebrite Commander** and Cellebrite Commander is indicated at the top of the screen.
5. Click **Save**.

> The license is validated against the license that exists in Cellebrite Commander, and any changes are taken from Cellebrite Commander.

15.10. Post-chain plugin

Add and remove plug-ins from the list of plug-ins that automatically run when you open a project. This can be useful when you have time constraints or large extraction files. These settings enable you to define whether or not to run certain plug-ins.



1. To add a plug-in to the list, click **Add Plugins** and select a plug-in from the list.
2. To remove a plug-in from the list of plug-ins that run automatically when you open a project, clear the check box in the **Enabled** column.
3. To remove a plug-in from the list, select the plug-in and click **Remove Plugins**.
4. To filter the plug-ins list, use the **Filter** box.

> The settings apply to subsequent projects opened in your current session. To save your configuration settings for use in subsequent sessions, see Saving settings (on the facing page).

15.11. Saving settings

Save your settings to reuse later, or to share with another user.

1. In the Settings window, click **Save Configuration**.
2. In the Save As window, browse to the location where you want to save your settings configuration, and click **Save**.

   The settings are saved as a Physical Analyzer Settings Configuration File (*.cnf).

15.12. Loading settings

Load your saved settings configuration.

1. In the Settings window, click **Load Configuration**.
2. In the Open window, browse to the location where your settings configuration is saved, select the configuration (*.cnf), and click **Open**.

   The settings are applied in the Settings window.

15.13. Setting project settings

Set unified time zone and case information for each project.

15.13.1. Setting a unified time zone for the project

During extraction, one time stamp per event is extracted.

For outgoing events, the time stamp is typically taken from one of the following sources:

- User-defined device time (where the device time has been manually set by the user: timestamps are displayed without the unified time (UTC).
- Network-defined device time (where the device time is automatically set by the network): timestamps are displayed with the unified time (UTC).

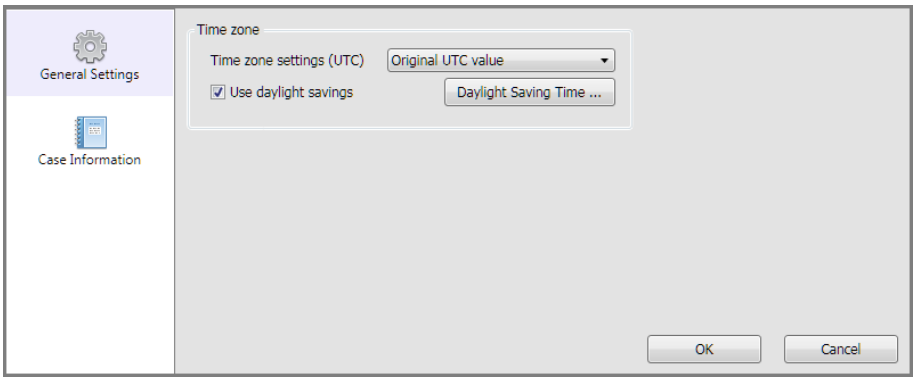
For incoming events, the time stamp is typically taken from the network-defined time (the time stamp assigned by the network); timestamps are displayed with the unified time (UTC).

Network-defined time stamps are subject to the time zones in which the event occurred.

Apply a unified time zone to the project to recalculate all network-defined time stamps according to the selected time zone in order to consolidate the events and view them sequentially in Physical Analyzer.

To apply a unified time zone to the project:

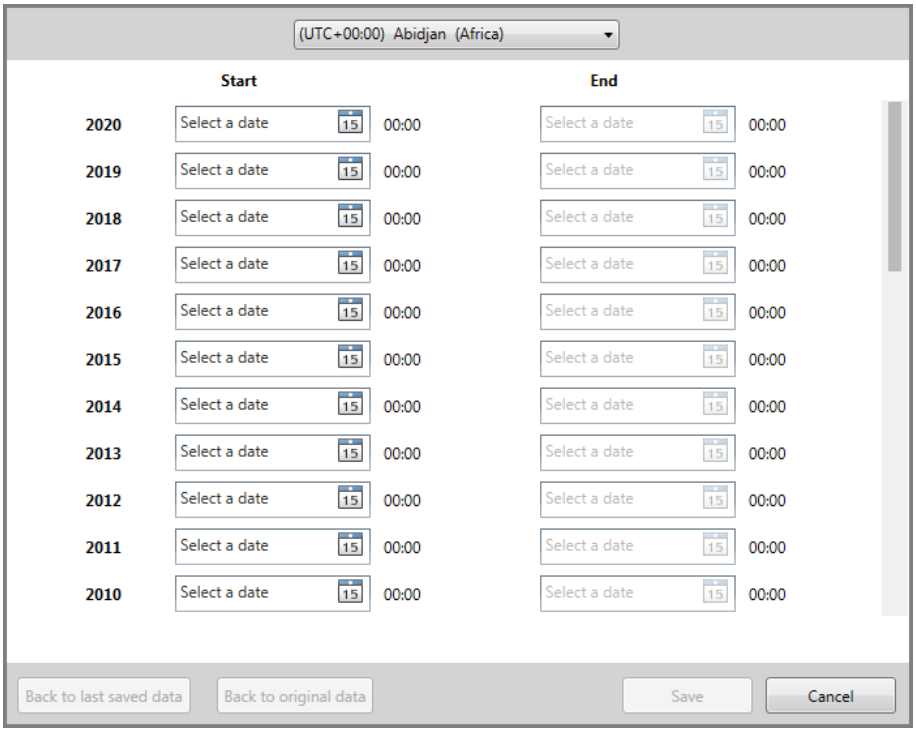
1. Do one of the following:
   - In the project **Extraction Summary** tab, click **Project settings**.
   - Go to **Tools > Project settings.**



2. From the **Time zone settings (UTC)** list, select:
   - **Original UTC value** to show time stamps as recorded.
   - One of the time zones (**UTC -12:00** to **UTC +13:00**) to recalculate network-defined time stamps according to the time zone offset.

> User-defined time stamps are not included in these recalculations, and are displayed as recorded.

3. To enable or disable the daylight saving time, select or clear the **Use daylight savings** check box.
4. To change the start and end dates for daylight saving time, click **Daylight Saving Time**.



a. For the year that you want to change, use the calendar to select the start and end dates, or edit the dates directly. You can use the button to remove certain years.

b. Click **Back to last saved data** to reset the table to the last time that you saved the data, click **Back to original data** to return the table to its default settings, or click **Save** to save the table with any changes that you made.

5. Click **OK**.

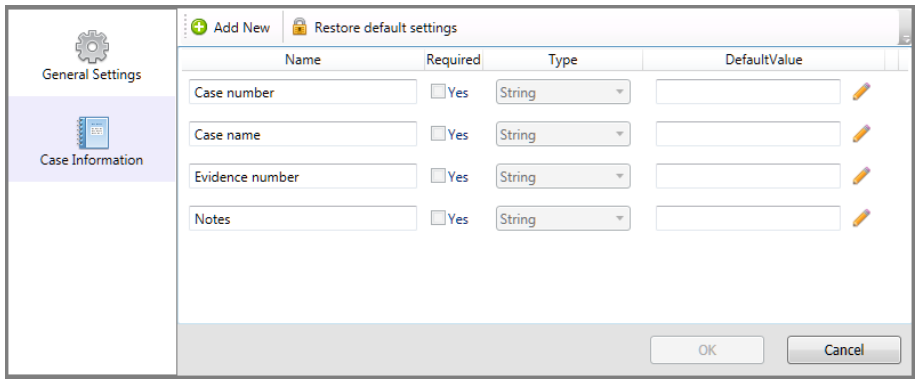
   The project is recalculated according to the selected unified time zone, and the new time zone is applied to the network-defined time stamps. Time stamps of events displayed in Physical Analyzer windows and any subsequently-generated reports reflect the selected unified time zone.

15.13.2. Setting the case information

Case information settings are saved with the project. The case number appears with the extraction information on the Welcome tab.

1. Do one of the following:
   - In the project **Extraction Summary** tab, click **Project settings**.
   - Click .

2. Go to **Tools > Project settings.**



3. Click **Add New**.

   Some case information fields appear by default.

4. Set the parameters for the default information fields:
   a. In the **Name** column, enter the relevant information (for example, case number, name, or notes).
   b. Select **Required** if this field must be filled.
   c. In the **Type** list, select one of the following:
      - **String** for text entry fields
      - **List** for a specified list of options
   d. In the **Default Value** box, set the default content:
      - For **String** type, type the default string. For a multi-line string, click , enter the default string in the Option Editor, and then click **OK**.
      - For a **List** type, click , enter the list items with each item on a separate line, then click **OK**.
5. To add more information fields, click **Add New**, and repeat step 3.
6. To remove the custom entries, click .
7. To restore the default settings, click **Restore default settings**.

16. Menus

This sections describes the menus and commands.

File menu (on the next page)

View menu (on page 451)

Tools menu (on page 452)

Extract menu (on page 454)

Python menu (on page 455)

Plug-ins menu (on page 456)

Report menu (on page 457)

Help menu (on page 458)

16.1. File menu

Open	Open a file for analysis using the standard analysis process.
Recent	Displays a list of recent projects.
Add external file	Include related artifacts in your case such as search warrants, additional images and relevant documents. See Adding external files (on page 77).
Add extraction to	Add an extraction to an open project.
Save as UFDX	Save a multiple extraction project as a UFDX file. This file enables the unified project to be opened as a single project with all its extractions.
Close tabs	Close all the tab windows for a specific project.
Close	Closes the currently active project.
Save project session	Saves the active project information generated by the user as a Physical Analyzer Session File (*.pas). See Saving a project session (on page 76).
Load project session	Loads a Physical Analyzer Session File (*.pas) onto an open project in the project tree.
Exit	Closes the Physical Analyzer and all active sessions.

16.2. View menu

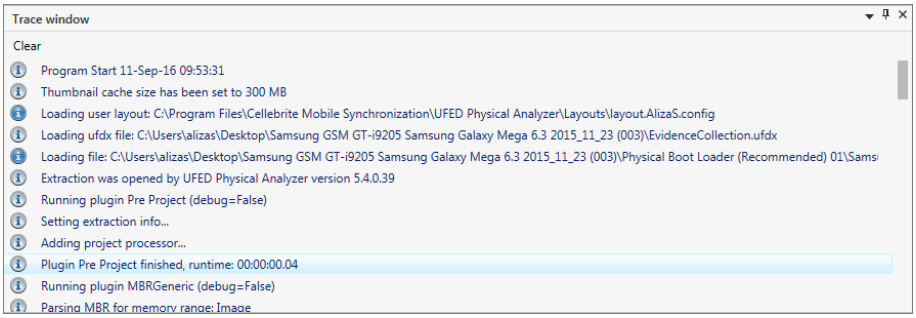
Welcome screen	Displays the **Welcome** tab. See Welcome tab (on page 97).
Trace window	Show/hide the trace panel at the bottom of the data display area.

16.2.1. Viewing the trace window

Show the Trace window at the bottom of the data display area to view a log of the actions performed in your session by you or by Physical Analyzer, such as plug-in activation.

1. In the **View** menu, select **Trace window**.

   The Trace window appears below the data display area.



2. To clear the log, in the Trace window, click **Clear**.
3. To close the Trace window, click ✕.

The Trace window can be hidden or displayed.

- To pin the Trace window open, click 📌.
- To unpin the Trace window, click ⊟.
- To view the Trace window when hidden, select or mouse over the tab.

16.3. Tools menu

Read Data from UFED	Enables data extraction directly to the computer.
Extraction file system	Exports and saves the parsed file system to actual files and folders in a directory structure. See Exporting the file system (on page 419).
Get more data (Carving)	**Carve images:** Opens the Carve Images window from where you can scan for images. See Carving images (on page 357). **Carve strings:** Opens the Carve Strings window from where you can scan for strings. **Carve locations:** Carve locations from unallocated space and unsupported databases. See Carving locations (on page 361).
Export account package	Extract an account package, which contains user credentials that can be imported into UFED Cloud .
Watch list	**Watch List Editor**: Opens the Watch List Editor, from where you can create, manage, and run your watch lists. See Accessing conversation view (on page 142). **Run Watch Lists on Active Projects:** Displays a list of active projects, from where you can apply watch lists. **Hash set manager:** Compare the MD5 hash sets of image and video files in an extraction to databases of known and blacklisted files. See Importing and categorizing hash sets (on page 152). **Export hash database:** Create an export file that includes a hash of offending photos that you can share with project VIC and CAID. See Exporting the hash database (on page 163).
Malware scanner	Opens the Malware scanner sub-menu, from where you can run malware detection on your extraction, and update the signature database. See Scanning for malware (on page 29).
Translation	Downloads the translation pack from the Internet, installs the translation pack from a file, or displays the supported languages. See Translating decoded data (on page 191).
Offline maps	Installs offline map packages. See Viewing offline maps (on page 174).
Enrichment of BSSID and cell IDs	Opens the Enrichment database sub-menu, from where you can install the database, import and export XML files with BSSID and cell tower data, as well as online enrichment. See Enrichment of BSSID and cell IDs (on page 178).
SQLite wizard	Opens the SQLite wizard sub-menu, from where you can open the SQLite wizard or select a SQLite database. See SQLite wizard (on page 307).
TomTom	Opens the TomTom sub-menu, from where you can export the TomTom extraction file and import the returned xml file. See Working with TomTom (on page 334).
Run fuzzy model plugin	Identify new data sources, handle and parse unknown databases. See Fuzzy models (on page 330).

Virtual Analyzer	Use the Virtual Analyzer to recover data from unsupported apps, view your data as if you were using the owner's device and validate decoded artifacts. See Virtual Analyzer (on page 288).
AppGenie	A research tool that provides additional app data such as Contacts, User accounts and Chats. SeeAppGenie (on page 285).
Manage tags	Opens the Manage tags window. See Tags (on page 167).
Manage public domain avatars	Create avatars to extract and preserve public domain, forensically sound data in one workflow. You can enrich your extracted data sources, and quickly reveal evidence hiding in plain sight on Facebook, Instagram and Twitter. See Accessing public data (on page 300).
Generate dictionary files	Create alphanumeric files with all the words in a decoded project. See Generating dictionary files (on page 333).
Settings	Opens the application settings window. See Settings.
Project settings	Set unified time zone and case information for each project. See Setting project settings (on page 445).

16.4. Cloud menu

Extraction > Private cloud data	Starts the UFED Cloud case wizard to extract private data from cloud data sources. See, Extracting private cloud account data (on page 208).
Extraction > Public cloud data	Starts the UFED Cloud case wizard to extract public data from cloud data sources. See, Extracting public cloud account data (on page 234).
Manage avatars	Manage public domain avatars.

16.5. Extract menu

iOS device extraction	Starts iOS device extraction to perform extractions from iOS devices. See Extraction from iOS devices (on page 269)
Extract GPS/mass storage device	Reads and saves data from GPS and mass storage devices connected to the workstation via USB connection. See Reading data from a GPS or mass storage device (on page 278).

16.6. Python menu

Python shell	Opens the Python shell window for user customer analysis using Python commands. See Using the Python shell (on page 418). For additional information on how to use Python shell commands for custom analysis, refer to the "Python Scripting Guide", accessible from the **Help** menu.
Run script	Runs a pre-written Python script (*.py file).
Run script (debug enabled)	Enables you to run a pre-written Python script (*.py file) in debug mode.

16.7. Plug-ins menu

Add/remove plug-ins	Displays the list of pre-installed plug-ins to enable management of the currently installed plug-ins. See Managing plug-ins (on page 416).
Run plug-in	Enables you to select a specific plug-in and run it. See Running a specific plug-in (on page 418).
Chain manager	Displays the Chain manager window to enable management and creation of device processing chains. See Managing chains (on page 404).

16.8. Report menu

Generate Report	Generates a report summary of all information found by the analysis process. See Generating a report (on page 257).
Generate preliminary device report	Generates an 'at a glance' intelligence report that includes parsed device information and user account information. See Generating a Preliminary device report (on page 268).

16.9. Help menu

Supported apps	Lists the supported applications and verified versions for Android, BlackBerry, iOS, and Windows Phone devices.
Manual	Opens the user manual.
Check for new version	Check for new software version if connected to the Internet.
Python shell scripting guide	Opens the Python Scripting Guide in PDF format.
View promotion	Displays information about the UFED Cloud application and the translation feature.
Learn more	Displays our latest capabilities and learn about other features.
Show license details	Displays the current software or hardware (dongle) license information, and enables you to: » Activate or load a new license (software or dongle) » Display information about previous dongles that were connected to this workstation » Deactivate a software license » Get direct access via email to Cellebrite support and sales
Zip log files	Zips the log files and opens the folder where the zipped log files are saved.
Zip log files with system information	Zips the log files and includes detailed information about the operating system, drivers, application data, event logs etc. This information can be used to analyze report cases.
License agreement	Opens the software license agreement.
About	Provides information about the installed Physical Analyzer version.

17. Glossary

A

Account package

An export file in .ucae format that contains user credentials, tokens or cookies, that can be imported and used to authenticate cloud accounts. An account package can be exported from Physical Analyzer, Cloud Login Collector and more.

Advanced logical extraction

An extraction method that combines both the logical and file system extractions into a single extraction method. This method helps users overcome the pain of long and convoluted extractions, saving time and effort while maintaining forensically sound data.

apk

Android application package file. Each Android application is compiled and packaged in a single file that includes all of the application's code (.dex files), resources, assets, and manifest file.

Apple File Conduit

AFC2. A service that is used by computer applications such as iTunes and iPhoto to read files from a device over USB.

Avatar

A social media profile that you can use to extract public data. Note: Avatars are public profiles, and as such, are exposed to public review.

C

CAID

Child Abuse Image Database. CAID sources images from police and NCA. Images are assigned unique identifiers – called hashes - and metadata. If CAID hashes appear in a case, they may indicate child abuse and/or exploitation.

Carve locations

Decodes additional location data from unallocated space and unsupported databases.

Carving

The process of finding data contained within the hexadecimal code, apart from what the forensic software has automatically offered. Carving can become necessary when the forensic tool parses data from unsupported apps, with deleted data including images, and other situations with file system and physical extractions.

CAS

Cellebrite Advanced Services (CAS) offers customers the ability to recover valuable evidence from heavily damaged, locked or encrypted devices.

Cellebrite Commander

Simplify how you manage and control all deployed devices and systems with the Cellebrite Commander. Reduce ongoing administration costs by remotely accessing devices and systems across your operation.

Cellebrite Pathfinder

Cellebrite Pathfinder is designed to afford users with the greatest opportunity currently possible to complete a near encyclopedic review of Big Data collections. Cellebrite Pathfinder is available in two versions: Desktop and Enterprise. The user-interface of each Cellebrite Pathfinder version is modeled to complete extensive reviews in a reduced time factor.

Cellebrite Reader

An application designed to allow users to view and share analysis reports with other authorized personnel, such as colleagues, other investigators, and attorneys.

Cellebrite UFED 4PC

Enables users to deploy extraction capabilities on Windows based tablets, laptops, and desktop computer systems. It performs physical, logical, file system and password extractions on a wide range of devices.

Cellebrite UFED Touch

Enables the simplified extraction of mobile device data. Depending on the license purchased, it performs physical, logical, file system and password extractions on a wide range of devices.

Chain

A chain is a set of plug-ins grouped together, which is used to process the extracted data of a device. Each device in the supported devices list of the application has a predefined parsing chain assigned to it. As part of its building blocks, a chain can also include other predefined chains.

Common/Known Image Filter

As part of the decoding process, UFED Physical Analyzer can calculate hash values of any extracted data file, particularly for media files. UFED Physical Analyzer automatically filters out common images. This saves time that would otherwise be spent reviewing common media images that are device files, image icons or images that are part of an app's installation.

D

Data source

The source of the extracted data (e.g., Facebook, Google Takeout, Dropbox).

Decoding

The process of translating raw hexadecimal data into an easily readable format. An automatic process within applications such as Physical Analyzer, decoding renders data easier for the examiner to find and analyze. From file system and physical extractions, the examiner always has the option to examine hexadecimal code within the raw data.

Dongle license

Is a software copy protection device that plugs into the USB port of the computer. Upon startup, the application looks for the key and will run only if the key contains the appropriate code.

F

Forensically sound

Extracted data is said to be forensically sound if it was collected, analyzed, handled, and stored in a manner that is acceptable by the law, and there is reasonable evidence to prove so. Forensic soundness provides reasonable assurance that extracted data was not corrupted or destroyed during investigative processes, whether on purpose or by accident.

G

Geodistance

The distance calculated between points which are defined by geographical coordinates in terms of latitude and longitude.

GPU

The Graphics Processing Unit (GPU) is a specialized processor that can rapidly execute commands for manipulating and displaying images. To boost media analytics speed in Analytics Desktop, it is recommended to add a GPU that matches or surpasses the minimum system requirements.

H

HashDB

Upload hash databases to compare them against the hash values in your cases. Hash databases leverage the use of extremely large and high quality hash sets to identify and eliminate images and videos. Using hash sets, law enforcement agencies are pre-categorizing or identifying images as part of a first-time sweep of seized evidence. CSV and TXT files as well as Project VIC, CAID and National Software Reference Library (NSRL) database formats are supported.

J

JTAG extraction

JTAG (Joint Test Action Group) is an advanced method of data extraction that requires a forensic examiner to connect to the test access ports of the device to obtain a full physical image. This enables the examiner to unlock and gain access to the raw data stored on the memory chip.

L

Location

Location data is drawn from different locations within the mobile device including Cell towers, WiFi networks, Harvested Cell towers, Harvested WiFi networks, Media locations, Favorites, Reminders, Home, Entered, TomTom, Foursquare, GpsFix, Recent, Frequent, Wireless networks

M

Markers

Markers signify the location where a person's device registered. The color of the marker signifies which person was registered at a particular location. At a low zoom

level, markers show the approximate location, and may include the data of more than one person.

O

Owner

The owner of the device that is the subject of the investigation.

P

Parties

Participants in a conversation. For example, communications such as instant messaging, emails, etc.

Physical/Logical Analyzer

An analysis and reporting tool for logical, file system and physical extractions. This software solution provides users with the capability to extract data, perform advanced analysis, decoding and reporting and presenting the results in a clear and concise manner.

Project tree

The area in UFED Physical Analyzer Tthat displays the extracted information structure of each project opened for analysis.

Project VIC

An ecosystem of information and data sharing between domestic and international law enforcement agencies combating sexual exploitation of children. Project VIC aims to compile all existing online child abuse images into a single repository. Each image and video frame is tagged with a unique identifier known as a "hash value." If a hash value from Project VIC appears in a case, it is an immediate indication that child sexual abuse may be involved.

Public data

Public activity on social media channels. UFED Cloud offers an option to capture public activity of a Facebook account or other popular apps. (Credentials not required.)

R

Rebuild cache

Reconstructs webpages, from cache files. You can view websites content offline with content from the browser cache (when available).

S

SQLite database

A database file format often used for data storage. Commonly used for storage of mobile and application data, but many smartphones may use .db files, .plists, and other file formats as well.

SQLite wizard

Visually decode additional data from databases, particularly from unfamiliar databases that were not decoded and may contain important case information.

State

State of a file indicates whether is was intact, deleted by the user or has an unknown status.

T

Tag

An investigator can apply a tag to flag events for future reference. Each event can have multiple tags. Tags can be included in reports or used for filtering.

Tokens

Username and password data as saved on a Windows computer.

Two-factor authentication

Referred to as two-step verification or dual factor authentication, is a security process in which the user provides two different authentication factors to verify themselves to better protect both the user's credentials and the resources the user can access.

U

UFDR

Universal Forensic Extraction Device Report

UFDX

UFED generates a UFDX file when there are multiple extractions for a device. It contains information about each extraction

UFED

Universal Forensic Extraction Device

Unallocated space

The area on a device's memory outside the defined file system that is available to write data to. Very often, deleted data or fragments can be found and carved from unallocated space.

V

Virtual Analyzer

The Virtual Analyzer enables you to view your data as if you were using the owner's device, validate decoded artifacts and recover data from unsupported apps. It requires an active UFED Physical Analyzer license. The Virtual Analyzer is based on

the Andy OS emulator, which is an external tool that simulates an Android device on your computer.

W

Watch lists

A list of keywords used to comb data for important and relevant information. Supports wildcards.

18. Index

A

Accessing conversation view 142

Activating the license 24

Adding a new data file type 430

Adding a new report field 436

Additional report fields 436

Addresses, retrieving 181

Advanced decoding 14, 404

Advanced features 280

Advanced opening of a non-UFED extraction file 49

Advanced opening of a UFED extraction file 42

Android backup 243, 255

Android Unlock Password Carver plug-in 420

Android Unlock Pattern Carver plug-in 419

Application menu 81

Attaching devices to a chain 409

Avatar, public data 305

B

Binary dump, adding 48

BlackBerry backup files 339

Browsing the file system 142

Browsing the Hex extraction 398

BSSID 178

BSSID, enrichment 261, 426, 439, 452

C

CAID 152

CAPTCHA 221

Capture 17, 126, 132, 137, 186

Capture images 298

Carved images 359

Carving images 357

Carving, generic 363

Carving, locations 361, 363

Changing the decoding chain 45

Chat bubbles 260, 439

Close tabs, unified project 72

Closing a project 79

Constructing a new chain 406

Content tab 72, 98

Conversation view 137

Creating a watch list 145

D

Data analysis 15

Data display area 81, 96

Data files 90, 260, 429-430, 434

Data files filtering methods 430

Data sources 209

Data tabs 106

Database view 106, 112

Decoding raw data 400

Deep carving, recover deleted records 427

Deleting a data file type 431

Deleting a report field 437

Deleting a watch list 148

Detaching devices from a chain 411

Detect false positives 427

Device Locations 179, 182

Device origin 172

Dictionary files 333, 424, 453

Dongle 22, 24-25

Dongle license 25

drone data 182

E

Editing a report field 437

Editing a watch list 147

Editing an existing chain 407

Editing an existing data file record 431

Export options 80, 87, 114, 138, 142, 147, 169, 180, 208, 233, 261, 328, 334, 379, 381, 383, 386, 388-389, 393, 395, 397, 399, 402, 423

Export the hash 163

Export, format 138

Exporting a TomTom file 334

Exporting a watch list 148

Exporting the file system 419

Extract files

all, selected 231

Extract menu 454

Extracting data from a device with a complex password 276

Extracting data from a device with a simple password 275

Extraction from GPS or mass storage devices 277

Extraction from iOS devices 269

Extraction summary tab 98

Extraction, rename 99

F

File Info tab 120

File menu 450

Files view 253

Folder view 106, 111, 125, 131

Fuzzy model 330

G

General settings 163, 168, 175, 181, 421, 439

Getting started 33

Global search results, tagging 141

GrayKey extractions 41

GriffEye, export format 138

H

Hash database 152

Hash values 76, 364

Help 191, 370, 373, 419, 442, 455, 458

Help menu 458

Hex data information 401

Hex view 90, 106, 112, 116, 118-119, 126, 132, 142, 375, 398, 400, 402

Hex viewer settings 432

Highlights database files 425

Highlights tab 119

I

IMAP data source 225

IMAP parameters 226

Importing a TomTom file 335

Importing a watch list 147

Installation and activation 17

Installation process, Virtual Analyzer 291

Interface language 204, 267, 422

Introduction 14

Investigation notes 266

iPhone calendar events, year 1604 269

J

JTAG 52, 70, 413, 419

L

Legal notices 2

Licensing 27, 191

Loading a project session 79

Loading settings 445

Locating a watch list 151

Locating and analyzing information 135

Locating specific data types in the Hex 402

Logical extraction 14

M

Malware 29

Managed connection, CMS 443

Managing chains 404

Managing data files settings 430

Managing hash sets 153

Managing plug-ins 416

Markers and information windows 177

Multiple extractions 433

Multiple projects 433

Multiple extractions 70

Multiple Extractions, filter 137

N

Network 27, 170, 369, 428, 445

Network dongle 27, 369

New version notification 24

Notification center 122

O

Offline maps 174

Offset jump to a different location in file 398

Online maps 171

online mode, Virtual Analyzer 289

Opening an extraction for analysis 33

Orientation to the workspace 81

P

Performing extractions 269

Performing physical extraction 270, 274

Performing physical extraction from encrypted devices 274

Performing physical extraction from non-encrypted iOS devices 270

Physical extraction 14, 42, 63, 183, 243, 269-270, 274, 294, 340, 357, 419

Plug-in, running a specific 418

Plug-ins 16, 376, 404, 416, 418, 456

Plug-ins menu 456

Premium languages 191

Prerequisites 269

Project tree 79

Project VIC 152

Project, rename 100

Public data 300

Python menu 455

Python Shell 418

R

Reading data from a GPS or mass storage device 278

Recover deleted data, carving 427

Redact, image or video 133

Removing a chain 412

Report defaults 438

Report menu 457

Running a watch list 149

S

Save, unified project 72

Saving a .ufd file 55

Saving a project session 76

Saving settings 445

Scanning for carved images 357

Scanning for malware 29

Screen capture 186

Screenshots 403

Search, jump to a location 172

Searching bytes 379

Searching dates 381

Searching for codes and passwords 396

Searching for information in a data tab 135

Searching for information in all open projects 140

Searching for information in the Hex data and decoded data 376

Searching for patterns 393

Searching for regular expressions (GREP) 388

Searching SIM ICCID numbers 384

Searching SMS numbers 386

Searching SMS text strings 391

Searching strings 377

Service 248

Setting a unified time zone for the project 445

Setting project settings 445

Setting the case information 447

Setting the default device chain 410

Settings 75, 135, 155, 175, 181, 204, 207, 260, 267, 282, 319, 333, 338, 367, 373, 421, 442, 445, 453

Settings, hash sets 424-425, 428

Shortcuts 90

SIM extraction 14

Single project 70

Specifications 2

Specify a network location 278, 414

Specifying a different device 44

Split UFDR 266

SQLite 427

SQLite queries 138, 307

Starting from a blank project 51

Starting with device selection 50

System requirements 17

T

Table view for analyzed data 111

Table view for data files 110

Tagging 85

Tags 167

Telegram, advanced options 231

Theme and table color 435

Timeline settings 434

Timeline view 82

Tools menu 452

Translating decoded data 191

Translation, basic pack 197

Two factor authentication 220

U

ufdx file 71, 403

Unallocated space 358

unified project 70

Unread messages 227

Update files, project VIC 162

Updating the signature database (online) 30

Updating the signature database from file (offline) 31

Using the quick filter 135

V

Values tab 118

Video recording 186

View menu 451

Viewing image files 124

Viewing the trace window 451

Virtual Analyzer 288

Virtual Analyzer, using 294

W

Warrant return 40, 62

Watch Lists 92, 150, 452

Welcome tab 97, 447

Wild cards, HEX search 376

Working in data tabs 107

Working with Hex data 106, 110, 116, 119-120, 126, 132, 375-377, 379, 381, 384, 386, 388, 391, 393, 396, 398-402, 432

Working with TomTom 38, 170, 277-278, 334-335, 452

Working with watch lists 145

Z

Zip file 427